



# **ESX Server**

## **CHECKLIST**

Version 1, Release 1.1

21 July 2008

**Developed by DISA for the DoD**

UNCLASSIFIED

This page is intentionally left blank.

<b>1. ESX SERVER REVIEW PROCESS .....</b>	<b>8</b>
1.1 ESX Server Checklist Organization.....	8
1.2 Requirements .....	8
1.3 Data Collection .....	9
1.4 Assessment Procedures.....	9
1.5 VMS ESX Server SRR Data Entry Procedures .....	10
1.5.1 Performing the Review .....	10
<b>2. VIRTUAL SERVER ADMINISTRATOR CHECKLIST .....</b>	<b>13</b>
ESX0010: ESX Server is not configured in accordance with the UNIX STIG.....	13
ESX0020: A .....	14
ESX0030: VMotion virtual switches are not configured with a dedicated physical network adapter.....	15
ESX0040: There is no dedicated VLAN or network segment configured for virtual disk file transfers.....	17
ESX0050: Permissions on the configuration and virtual disk files are incorrect .....	19
ESX0060: iSCSI VLAN or network segment is not configured for iSCSI traffic .....	20
ESX0070: CHAP authentication is not configured for iSCSI traffic .....	22
ESX0080: iSCSI storage equipment is not configured with the latest patches and updates .....	24
ESX0090: iSCSI passwords are not in accordance with DoD policy.....	25
ESX0100: Static discoveries are not configured for hardware iSCSI initiators .....	26
ESX0110: USB drives load automatically when inserted into the ESX Server .....	28
ESX0120: The ESX Server does not meet the minimum requirement of two network adapters .....	29
ESX0130: The service console and virtual machines are not on dedicated VLANs or network segments.....	30
ESX0140: Notify Switches feature is not enabled to allow for notifications to be sent to physical switches .....	31
ESX0150: The ESX Server external physical switch ports are configured to VLAN 1.....	33
ESX0160: Permissions have been changed on the /usr/sbin/esxcfg-* utilities.....	34
ESX0170: Virtual machines are connected to public virtual switches and are not documented .....	36
ESX0180: Virtual switch port group is configured to VLAN 1 .....	37
ESX0190: Virtual switch port group is configured to VLAN 1001 to 1024 .....	39
ESX0200: Virtual switch port group is configured to VLAN 4095 .....	41
ESX0210: Port groups are not configured with a network label .....	43
ESX0220: Unused port groups have not been removed .....	45
ESX0230: Virtual switches are not labeled .....	47
ESX0240: Virtual switch labels begin with a number.....	49
ESX0250: The MAC address change 'Policy' is set to Accept for virtual switches.....	51
ESX0260: Forged Transmits are set to Accept for on virtual switches.....	52
ESX0270: Promiscuous Mode is set to Accept on virtual switches .....	54
ESX0290: External physical switch ports configured for EST mode are configured with spanning-tree enabled .....	57
ESX0300: The non-negotiate option is not configured for trunk links between external physical switches and virtual switches in VST mode.....	58

ESX0310: Undocumented VLANs are configured on ESX Server in VST mode .....	60
ESX0320: ESX Server firewall is not configured to High Security .....	60
ESX0330: A third party firewall is configured on ESX Server .....	63
ESX0340: IPtables or internal router/firewall is not configured to restrict IP addresses to services.....	64
ESX0350: ESX Server required services are not documented .....	65
ESX0360: ESX Server service console users are not documented.....	66
ESX0370: Hash signatures for the /etc files are not stored offline.....	67
ESX0380: Hash signatures for the /etc files are not reviewed monthly .....	69
ESX0390: The setuid and setgid flags have been disabled.....	70
ESX0400: ESX Server is not authenticating the time source with a hashing algorithm .....	72
ESX0410: ESX Server does not record log files .....	73
ESX0420: ESX Server log files are not reviewed daily .....	75
ESX0430: Log file permissions have not been configured to restrict unauthorized users ...	77
ESX0440: ESX Server does not send logs to a syslog server .....	78
ESX0450: Auditing is not configured on the ESX Server.....	80
ESX0460: The IAO/SA does not subscribe to vendor security patches and update notifications.....	81
ESX0470: The ESX Server software version is not at the latest release .....	82
ESX0480: ESX Server updates are not tested .....	83
ESX0490: VMware tools are not used to update the ESX Server .....	84
ESX0500: ESX Server software version is not supported.....	85
ESX0510: VMware and third party applications are not supported .....	87
ESX0520: There are no backup and recovery procedures.....	90
ESX0530: The ESX Servers and management servers are not backed up .....	91
ESX0540: Disaster recovery plan does not include virtual infrastructure.....	92
ESX0550: Backups are not located on separate logical partition from production data .....	92
ESX0560: VI client sessions to the ESX Server are unencrypted .....	93
ESX0570: VI Web Access sessions to the ESX Server are unencrypted .....	94
ESX0580: VirtualCenter communications to the ESX Server are unencrypted.....	95
ESX0590: SNMP write mode is enabled on ESX Server.....	96
ESX0600: VirtualCenter server is hosting other applications. ....	97
ESX0610: Patches and security updates are not current on the VirtualCenter Server. ....	99
ESX0650: VirtualCenter virtual machine is not configured in an ESX Server cluster with High Availability .....	101
ESX0660: VirtualCenter virtual machine does not have a CPU reservation.....	102
ESX0670: VirtualCenter virtual machine does not have a Memory reservation.....	103
ESX0680: CPU alarm is not configured.....	104
ESX0690: Memory alarm is not configured .....	105
ESX0700: Unauthorized users have access to VirtualCenter virtual machine .....	106
ESX0710: No dedicated VirtualCenter administrator created within the Windows Administrator Group .....	107
ESX0720: No logon banner warning is configured.....	108
ESX0730: VI Client sessions with VirtualCenter are unencrypted.....	110
ESX0740: VI Web Access sessions with VirtualCenter are unencrypted.....	111
ESX0750: VirtualCenter vpxuser has been modified .....	112

ESX0760: Users assigned to VirtualCenter groups are not documented .....	113
ESX0770: Users are not documented in the Windows Administrators group.....	114
ESX0780: VirtualCenter Server groups are not reviewed monthly.....	115
ESX0790: No documented configuration management process exists for VirtualCenter changes.....	116
ESX0800: There is no VirtualCenter baseline configuration document .....	117
ESX0810: VirtualCenter does not log user, group, permission, or role changes .....	118
ESX0820: VirtualCenter logs are not reviewed daily.....	119
ESX0860: There is no up-to-date documentation of the virtualization infrastructure.....	119
ESX0863: ESX Server is not properly registered in VMS .....	120
ESX0866: ESX Server assets are not configured with the correct posture in VMS.....	121
ESX0869: VirtualCenter Server assets are not properly registered in VMS .....	122
ESX0872: VirtualCenter Server assets are not configured with the correct posture in VMS. ....	123

### **3. VIRTUAL MACHINE ADMINISTRATOR CHECKLIST..... 124**

ESX0880: ISO images are not restricted to authorized users .....	124
ESX0890: ISO images do not have hash checksums.....	125
ESX0900: ISO images are not verified for integrity .....	126
ESX0910: Master templates are not stored on a separate partition .....	127
ESX0920: Master templates are not restricted to authorized users only .....	128
ESX0930: The VMware-converter utility is not used for VMDK imports or exports .....	129
ESX0940: Nonpersistent disk mode is not set for virtual machines.....	130
ESX0950: No policy exists to assign virtual machines to personnel.....	131
ESX0960: VI Console is used to administer virtual machines .....	132
ESX0970: Clipboard capabilities are enabled for virtual machines .....	132
ESX0980: VMware Tools drag and drop capabilities are enabled.....	134
ESX0990: The VMware Tools setinfo variable is enabled for virtual machines .....	135
ESX1000: Configuration tools are enabled for virtual machines .....	137
ESX1010: Virtual machines are not time synchronized .....	138
ESX1020: The IAO/SA does not document and approve virtual machine renames .....	140
ESX1030: Test and development virtual machines are not logically separated from production virtual machines.....	141
ESX1040: No policy exists to restrict copying or sharing virtual machines over networks and removable media .....	142
ESX1050: Virtual machine moves are not logged.....	143
ESX1060: Virtual machine moves to removable media are not documented .....	144
ESX1070: Virtual machines are removed from the site without approval documentation .....	144
ESX1080: Production virtual machines are not located in a controlled access area .....	145
ESX1090: Virtual machine rollbacks are performed when virtual machine is connected to the network.....	146
ESX1100: Virtual machine OS log files are not saved before rollback .....	147
ESX1110: Virtual machine log files do not have a size limit.....	148
ESX1120: ESX Server is not configured to maintain a specific number of log files .....	149
ESX1130: Virtual machine log files are not retained for 1 year.....	151
ESX1140: Virtual machines are not backed up .....	152
ESX1150: Virtual machines are not registered in VMS .....	153

<b>4. GUEST ADMINISTRATOR CHECKLIST .....</b>	<b>154</b>
ESX1160: Virtual machine requirements are not documented.....	154
ESX1170: Unused hardware is enabled in virtual machines .....	155
ESX1180: Guest operating system selection does not match installed OS .....	156
ESX1190: Guest operating system is not supported by ESX Server.....	157
ESX1200: Anti-virus software and signatures are out of date for off and suspended virtual machines. ....	164
ESX1210: OS patches and updates are out of date on off and suspended virtual machines .....	165

This page is intentionally left blank.

## 1. ESX SERVER REVIEW PROCESS

### 1.1 ESX Server Checklist Organization

Management of the VMware Infrastructure is typically performed by several users performing different roles. The roles assumed by administrators are the Virtualization Server Administrator, Virtual Machine Administrator, and Guest Administrator. VMware Infrastructure users may have different roles and responsibilities; however some functional overlap may occur. The ESX Server Checklist is formatted around these roles to better facilitate the use of the document and provide easy access to specific information pertaining to the administrator's role or responsibility. These roles are defined to provide role responsibilities and organize the ESX Server Checklist requirements in this document.

**Virtual Server Administrator** - This role is responsible for installing and configuring the ESX Server hardware, storage, physical and virtual networks, service console, and management applications.

**Virtual Machine Administrator** - This role is responsible for creating and configuring virtual machines, virtual networks, virtual machine resources, and security policies. The Virtual Machine Administrator creates, maintains, and provisions virtual machines, and virtual networks through VirtualCenter.

**Guest Administrator** - This role is responsible for managing a guest virtual machine or machines. Tasks that are typically performed by Guest Administrators are connecting virtual devices, system updates, and applications that may reside on the operating system.

**Note:** Three vulnerabilities that are in the ESX Server STIG are not included in this checklist, since this checklist is only applies to ESX Server 3. Checks ESX0830, ESX0840, and ESX0850 only apply to ESX Server 3i. These checks will be addressed in a separate checklist for ESX Server 3i.

### 1.2 Requirements

The following section presents the data collection and analysis methodology for a ESX Server Security Readiness Review (SRR). The items reviewed as part of this SRR are based upon the requirements published by DoD Directive (DoDD) 8500.1, paragraph 4.18. The DoD Directive, DoDD 8500.1 requires guidelines to be developed by DISA FSO in accordance with DoD-approved security configuration as specified in the DoD Directive O-8530.1

The requirements to perform an ESX Server SRR are as follows:

- *ESX Server Security Technical Implementation Guide* – The ESX Server STIG will assist the reviewer with further detail in performing the ESX Server checks. The ESX Server STIG may be downloaded from the IASE web site located at <http://iase.disa.mil>.



- *ESX Server SRR Checklist* - A comprehensive list of checks that provide step-by-step procedures on performing an ESX Server SRR. The checklist may be downloaded from IASE web site located at <http://iase.disa.mil>.
- User access to the Vulnerability Management System (VMS) which is located at <https://vms.disa.mil/VMSMain.asp>
- The review team will need an OS, Application Server, and Database reviewer to review all the components of the ESX Server system.

### 1.3 Data Collection

The initial data collection is achieved through the ESX Server SRR Checklist. The checklist provides the details and procedures for evaluating ESX Servers and their potential security vulnerabilities. Listed below are the general steps involved in performing an ESX Server SRR.

1. Prior to arriving onsite, acquire the latest printed copy of the ESX Server Checklist and latest UNIX SRR CD.
2. Ensure that you have a valid VMS account.
3. If possible, acquire a current copy of the sites ESX Server topology (network diagram) prior to arriving on site or obtain a copy as soon as possible after arriving on site.
4. During or soon after the in-brief at the site, obtain the names and phone numbers of the onsite POCs for the ESX Server review.

### 1.4 Assessment Procedures

The reviewer is responsible for coordinating with site personnel in arranging the review of the site's network. Listed below are the procedures for the collection of SRR data:

1. Interview the System Administrators/IAOs, either individually or as a group, to complete the SRR ESX Server Architectural and Policy (Non-computing) and ESX Server Computing checks.
2. The Team Lead will create a Vulnerability Management System (VMS) Visits folder and provide the visit names to the reviewer.
3. After all of the data for the ESX Server SRR is collected and the ESX Server Checklist is complete, then enter the information into VMS.
4. Enter the ESX Server SRR results into the proper VMS visit by cross referencing the Vulnerability ID with the STIG ID located on the ESX Server SRR Checklist.
5. Upon the completion of entering the vulnerabilities into VMS, the reviewer will verify that no vulnerabilities are in the Not Reviewed (NR) status. Any Not Reviewed vulnerabilities will be reviewed again to ensure it has been entered correctly.

6. Open findings will be reviewed to ensure the “Finding Details” field has accurate text. If the “Finding Details” field is empty, the reviewer will enter appropriate text explaining the cause of the Open Finding.
7. A Severity Code can be downgraded to a lower category on an Open Finding only if DISA FSO ESX Server Checklist has provided documentation allowing that particular vulnerability to be downgraded. The downgraded finding will meet the allowable mitigations specified in the documentation. In addition, all downgraded vulnerabilities will contain a reason why it is being downgraded.
8. The reviewer will discuss with the site personnel the feasibility of closing all Category I findings before the team leaves the site. The reviewer will keep the Team Lead informed of all Category I findings and provide additional emphasis and clarity when explaining why some Category I findings cannot be closed immediately.
9. Floppy disks, CDs, USB drives, data entry forms, and reports will be handled and protected in accordance with their level of classification.
10. The reviewer will communicate to the Team Lead the status of VMS data entry through the daily meetings and will send an email to the Team Lead only if the VMS data entry cannot be completed on site.

## **1.5 VMS ESX Server SRR Data Entry Procedures**

### **1.5.1 Performing the Review**

Verify the asset is registered in VMS under the correct organization. Assets not registered will need to be created. When creating the asset, the asset ownership defaults to the person creating the asset. It is recommended that the SA create the asset. If the reviewer creates the asset the permissions will need to be reassigned to the SA.

#### **1. Creating the Asset**

1. Expand Asset Findings Maintenance
2. Expand Assets/Findings
3. Expand Visits to display sub-folders. *(Reviewer Only) SA will expand Location.*
4. Expand the sub-folder assigned. Each subfolder represents individual visits in VMS assigned for review.
5. Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing, and CNDS.

#### **1.1 Creating Non-computing asset**

1. Click the yellow folder icon located at the right of ‘Non-Computing’.
2. Click the General tab

3. Enter the Display name. The standard name for network non-computing asset will be: "SiteName\_ESX\_Policy"
4. Verify "Location"
5. Verify "Owner": Used to register asset to parent or child location.
6. Verify "Managed By": Used for remote locations being managed.
7. Verify Mac level, Confidentiality, & Classification is correct.
8. Click the 'Asset Posture' tab to add functions to the asset
9. Expand Non-computing
10. Expand 'Application'
11. Click 'ESX Architecture and Policy'
12. Click '>>' to move it to the 'Selected' window
13. Click the Systems / Enclaves tab
14. For registered enclaves, choose the correct enclave.
15. If the enclave is not present, ensure that the IAM or Team Lead works with the appropriate site personnel to request an enclave.
16. Click 'Save'

## **1.2 Creating Computing asset**

1. Click the Create Icon located next to computing. The asset form is displayed.
2. Click the General tab and enter the information into the required fields.
3. Click the asset identification tab and enter the IP address, MAC address and click add.
4. Click the Asset Posture Tab and drill down to select the following functions:
  - Operating System, Unix, VMware, ESX Server 3.
5. Click the '>>' to move it to the 'Selected window'
6. Click Save

## **2. Reassign Permissions for Asset (If Required)**

1. Expand Permissions
2. Click Reviewer Asset Update
3. Select Visit and submit
4. Select Asset and submit
5. Select User and submit

## **3. Procedures for Review of the Asset**

If all registration tasks have been accomplished, use the following procedures:

1. Expand Asset Findings Maintenance
2. Expand Assets/Findings
3. Expand Visits to display sub-folders. *(Reviewer Only) SA will expand Location.*
4. Expand the sub-folder assigned. Each subfolder represents individual visits in VMS assigned for review.
5. Expand the visit and display the location summaries. Within the location, assets are divided into computing, non-computing, and CNDS.

6. Expand 'Non-Computing' and 'Computing'.
7. Expand 'Must Review' (*Reviewer Only*) SA will not see 'Must Review'. If an asset was just created it would reside in 'Not elected for Review' section. Have the Team Lead move the asset to 'Must Review'.
8. Expand Asset to review. Ready to review is colored in RED Note: When you drill down into the asset you will find Vulnerabilities assigned to the ESX Server component and IAVMs when the OS is expanded.
9. Expand the ESX Server component and each Vulnerability Key.
10. Update the 'Status' of the vulnerability
11. Identify details on all open vulnerabilities
12. System Administrators will need to update the POA&M prior to saving.
13. System Administrators should expand the OS assigned to the asset and each IAVM. Verify the OS level meets the required release or patch level. Asset must be in the same status such as 'Open'
14. Save the updates to the asset.

#### **4. Verify that all necessary assets were reviewed**

1. Select Asset Findings Maintenance
2. Expand Assets/Findings
3. Expand visits to display the sub-folders
4. Expand the sub-folder assigned
5. Expand the visit and display the location summaries. Within the location, assets are divided into computing, non-computing, and CNDS
6. Expand 'non-computing'.
7. Expand 'Computing'
8. Expand 'Must Review' (If checkmarks are gone, the asset has been reviewed.)

#### **5. Add Comments**

1. Select Visit Maintenance
2. Expand Organization for the visit.
3. Expand Visit
4. Locate the visit.
5. Click on CCSD or enclave name.
6. Comments Tab – Add comment
7. Save Changes

#### **6. Compliance Monitoring**

1. Select Reports
2. VC06 – Asset Compliance Report
3. Can select an asset or an org
4. Select "open" status
5. Can sort on different fields

6. Display (Finding Comments, Finding Long Name, Finding Details, Vulnerability Discussion)
7. The AS01 report assists the reviewer or SA by quickly identifying the assets at the location the review is being performed. In the section “Looking at Network Assets” is a quick step by step instruction in creating the report. The site may want to do other reports, if your site manages or owns assets, which are not located at the site. Check Child Locations if applicable. Navigate to the Reports menu, Select the AS01 Report, and select the desired criteria for the report.
8. The VL03 report assists the reviewer or SA by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. Navigate to the Reports Menu, Select the VL03 Report, and select the desired criteria for the report.

## 2. VIRTUAL SERVER ADMINISTRATOR CHECKLIST

This role is responsible for installing and configuring the ESX Server hardware, storage, physical and virtual networks, service console, and management applications.

**ESX0010:** ESX Server is not configured in accordance with the UNIX STIG.

**Vulnerability Key:** V0015783

**STIG ID:** ESX0010

**Vulnerability:** ESX Server is not configured in accordance with the UNIX STIG.

**IA Controls:** DCCS-1, DCCS-2 Security Configuration Guide, ECSC-1 Security Configuration Guidance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The UNIX SRR scripts must be run first against all ESX Servers, since the ESX Server service console is considered a modified Linux distribution. DISA Field Security Operations has developed the UNIX SRR scripts to evaluate all UNIX machines against the UNIX STIG requirements. The UNIX SRR scripts determine all the open operating system vulnerabilities.

**Computing Check:** On the ESX Server service console, perform the following command:  
#find / -name Script.\*

If the command brings back an output, review the result files that are located under Script.(Month)/hostname. Review the results and verify that only GEN003540 and GEN006640 are open. If any other findings are open, then this is a finding.

If the command does not return a result, then the reviewer will have to run the UNIX SRR scripts from the CD. If there are any open findings other than GEN003540 and GEN006640, then this is a finding.

The following open findings will NOT be applicable when running the UNIX SRR against the ESX Server service console:

GEN003540 - Executable Stack

GEN003540 (CAT II) OPEN

FINDING DESCRIPTION GEN003540: The SA will ensure the executable stack is disabled.

SYSTEM CONFIGURATION: VMware ESX Server 3 does not support this configuration. The kernel has executable stack enabled.

GEN006640 - Virus Protection

GEN006640 (CAT I) OPEN

FINDING DESCRIPTION GEN006640: An approved DoD virus scan program is not used and/or updated.

SYSTEM CONFIGURATION: Unable to install McAfee Virus scan command-line tool on VMware ESX. Some of the prerequisite filesets for this product conflict with the versions required by VMware Operating System filesets.

**Fix:** Run the UNIX SRR scripts against the ESX Server service console.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0020:** An NFS Server is running on the ESX Server host

**Vulnerability Key:** V0015784

**STIG ID:** ESX0020

**Vulnerability:** An NFS Server is running on the ESX Server host.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Datastores may have several types of file system formats. These include VMFS, Raw Device Mappings, and NFS. VMFS is a proprietary file system developed by VMware that is built to handle a high amount of I/O generated by the ESX Server. Raw Device Mappings (RDM) is a mapping file in a VMFS volume that acts as a proxy for a raw physical device. An RDM can be thought of as a symbolic link from a VMFS volume to a raw LUN. An NFS volume is located on an NFS server. In normal usage there should be no case where an ESX host would be required to export an NFS directory or directories using an NFS server. If such a server were to exist within the ESX host operating environment, sensitive data from datastores to which the ESX server is attached may become compromised. Since there should never be a need for an ESX server to export a file system, the presence of a running NFS server is a finding.

**Computing Check:** On the ESX Server service console, perform the following:  
`#ps -ef | grep nfsd`

If you see the something other than the “grep nfsd” process, then this is a finding.

**Fix:** Do not configure an NFS Server on the ESX Server host.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0030:** VMotion virtual switches are not configured with a dedicated physical network adapter

**Vulnerability Key:** V0015785

**STIG ID:** ESX0030

**Vulnerability:** VMotion virtual switches are not configured with a dedicated physical network adapter.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

## **References:** ESX Server STIG

## **Severity:** Category II

**Vulnerability Discussion:** The security issue with VMotion migrations is that the encapsulated files are transmitted in plaintext. Plaintext provides no confidentiality, and anyone with the proper access may view these files. To mitigate this risk, a dedicated VLAN will be used for all VMotion migrations. Configuring a dedicated VLAN requires that VMotion virtual switches are configured with one physical network adapter on a separate VLAN. This will ensure that VMotion traffic is separate from production traffic. The preferred method to transfer these encapsulated files is to encrypt them with a FIPS 140-2 encryption algorithm.

## **Computing Check:**

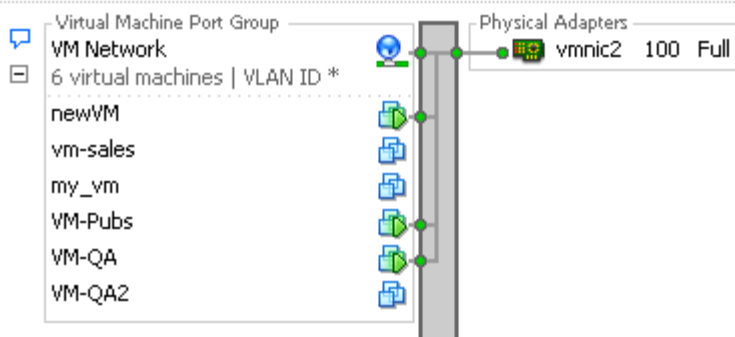
1. Log into VirtualCenter with the VI Client and select the server from the inventory panel.  
The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Examine the virtual switches and their respective VLAN IDs. A separate and dedicated physical network adapter should be configured for VMotion migrations to and from VMFS volumes. If there is no dedicated physical network adapter for these transfers, then this is a finding. To illustrate a dedicated physical network adapter the figure below shows the service console configured on a separate physical network adapter.



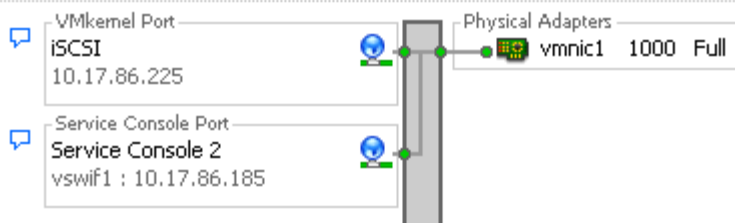
Virtual Switch: vSwitch0



Virtual Switch: vSwitch1



Virtual Switch: vSwitch2



**Caveat:** This check is Not Applicable if all the network adapters are configured as a NIC Team.

**Fix:** Configure a dedicated physical network adapter for all VMotion virtual switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0040:** There is no dedicated VLAN or network segment configured for virtual disk file transfers

**Vulnerability Key:** V0015786

**STIG ID:** ESX0040

**Vulnerability:** There is no dedicated VLAN or network segment configured for virtual disk file transfers.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

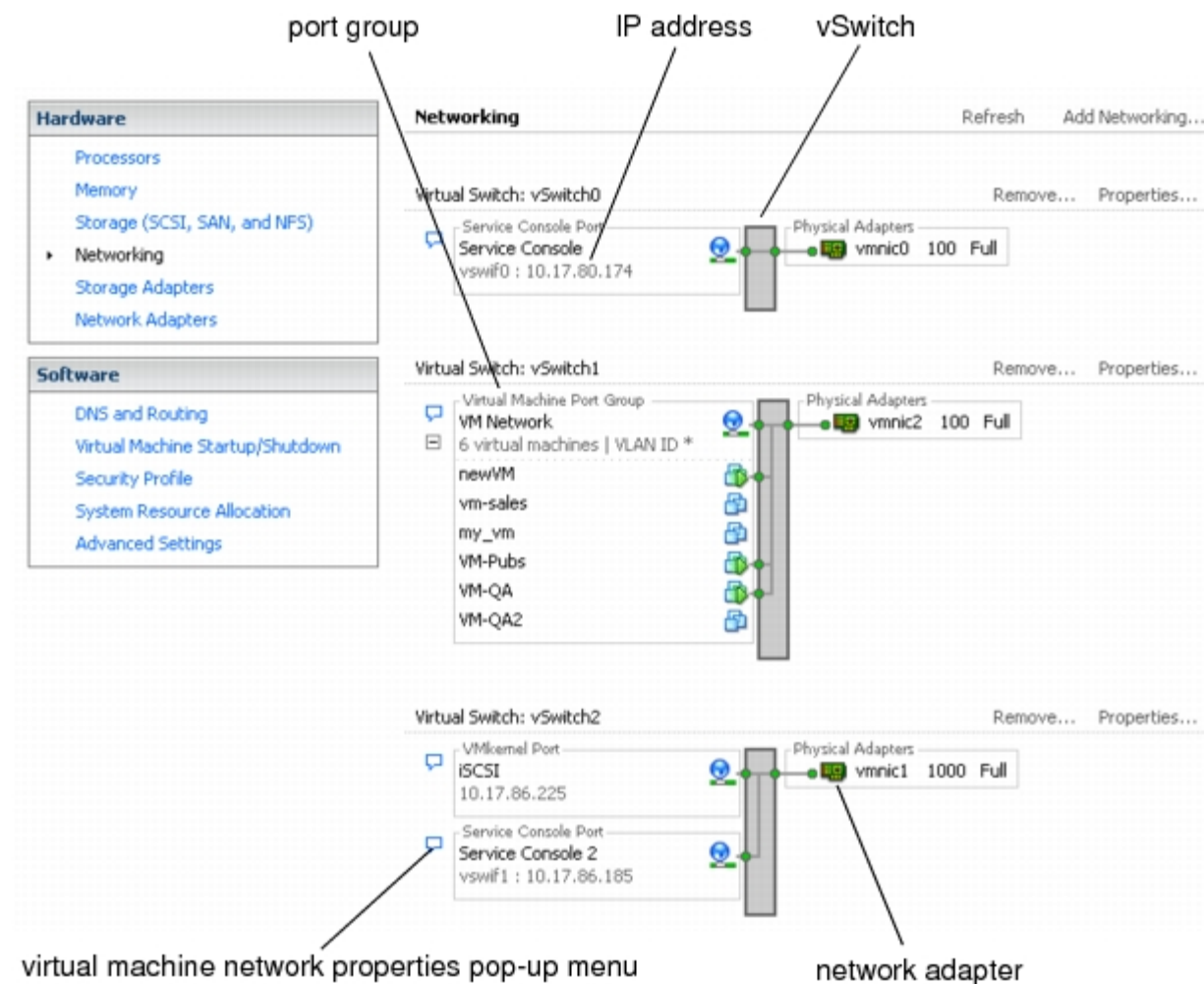
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The transfer of virtual disk files and VMotion migrations to and from VMFS volumes is sent in plaintext. This type of traffic provides no confidentiality for the data. Due to this vulnerability, at a minimum, virtual disk file transfers and VMotion migrations will be sent over a dedicated VLAN. The preferred method for these transfers is to encrypt this traffic with a FIPS 140-2 encryption algorithm.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel. The hardware configuration page for the server appears.
2. Click the Configuration tab, and click Networking.
3. Examine the virtual switches and their respective VLAN IDs. A separate and dedicated VLAN should be configured for virtual disk transfers and VMotion migrations to and from VMFS volumes. The administrative VLAN or Out of Band VLAN is acceptable for compliance. If there is no dedicated VLAN for these transfers, then this is a finding. To illustrate a dedicated VLAN, the figure below shows the service console configured on a separate VLAN (vSwitch0).



**Fix:** Implement a dedicated VLAN for all virtual disk file transfers to and from VMFS volumes.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0050:** Permissions on the configuration and virtual disk files are incorrect

**Vulnerability Key:** V0015787

**STIG ID:** ESX0050

**Vulnerability:** Permissions on the configuration and virtual disk files are incorrect.

## IA Controls: ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Permissions for the virtual machine files will adhere to VMware's best practices. The configuration file (.vmx), will be read, write, execute (rwx) for owner and read and execute (r-x) for group and read (r--) for others (754). The virtual machine's virtual disk (.vmdk) will be read and write (rw-) for owner (600).

**Computing Check:** On the ESX Server host, perform the following commands on the service console:

```
#find /vmfs -type f -name '*.vmx' -exec ls -Al {} \; | grep -v -- "rwxr-xr--"
```

Review the results from this command. If the result has permissions that are more restrictive, then this is not a finding. Any result that has less restrictive permissions (greater than 754) is a finding. If no result is returned, then this is not a finding. Permissions for all .vmx files should be 754 or rwxr-xr-- or more restrictive.

```
#find /vmfs -type f -name '*.vmdk' -exec ls -Al {} \; | grep -v -- "rw-----"
```

Any result from this command is a finding. If no result is returned, then this is not a finding. Permissions for all .vmdk files should be 600 or rw-----. If they are not, then this is a finding.

**Fix:** Configure .vmx to 754 and .vmdk to 600.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0060:** iSCSI VLAN or network segment is not configured for iSCSI traffic

**Vulnerability Key:** V0015788

**STIG ID:** ESX0060

**Vulnerability:** iSCSI VLAN or network segment is not configured for iSCSI traffic.

## **IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

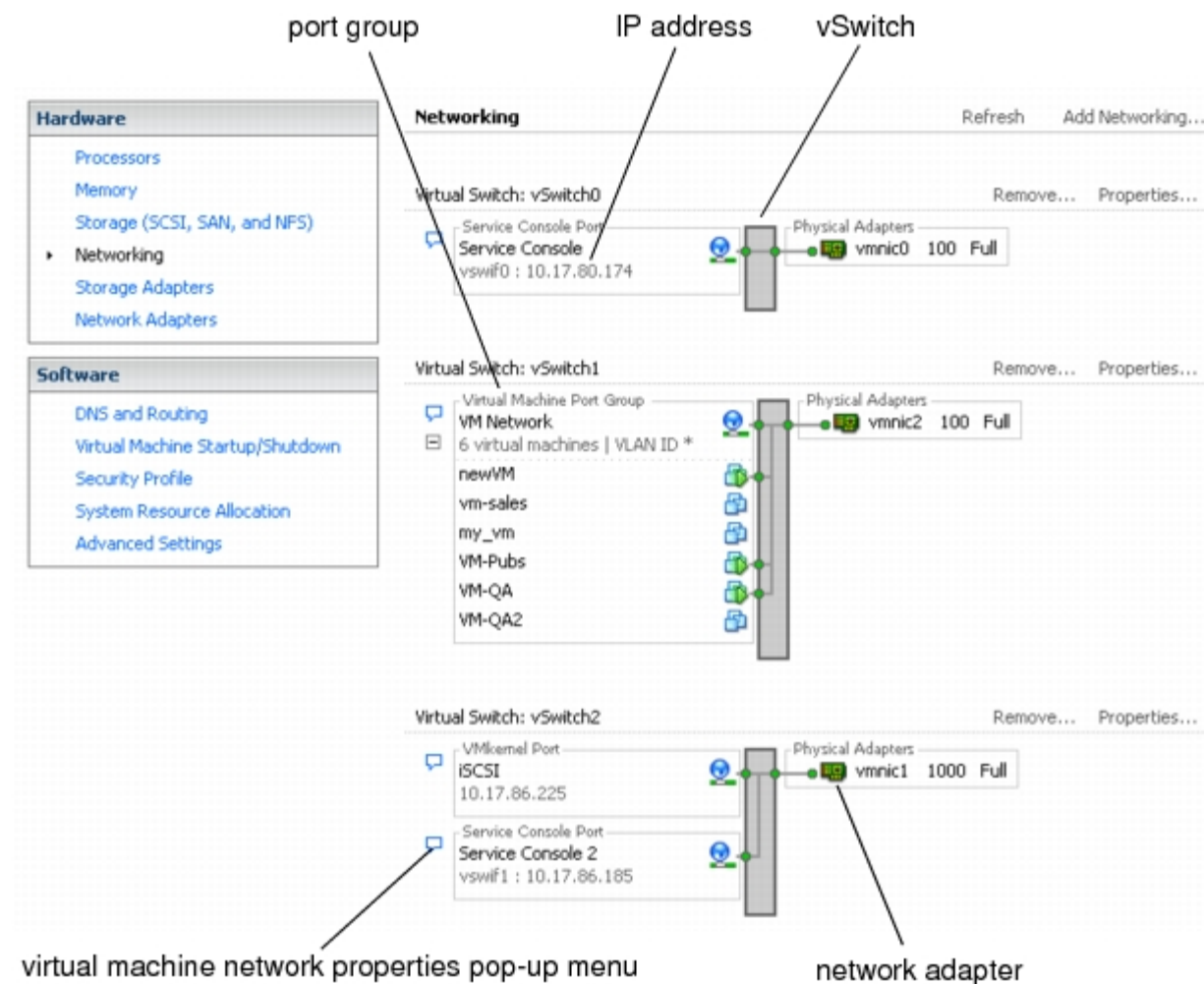
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines may share virtual switches and VLANs with the iSCSI configuration. This type of configuration may expose iSCSI traffic to unauthorized virtual machine users. To restrict unauthorized users from viewing the iSCSI traffic, the iSCSI network should be logically separated from the production traffic. Configuring the iSCSI adapters on separate VLANs or network segments from the VMkernel and service console will limit unauthorized users from viewing the traffic.

### **Computing Check:**

1. Log into VirtualCenter with the VI Client and select the server from the inventory panel.  
The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Examine the virtual switches and their respective VLAN IDs. A separate and dedicated VLAN should be configured for all iSCSI connections. If there is no dedicated VLAN for iSCSI, then this is a finding. To illustrate a dedicated VLAN, the figure below shows iSCSI configured on a separate VLAN (vSwitch2).



**Fix:** Configure a dedicated VLAN or network segment for iSCSI connections.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0070:** CHAP authentication is not configured for iSCSI traffic

**Vulnerability Key:** V0015789

**STIG ID:** ESX0070

**Vulnerability:** CHAP authentication is not configured for iSCSI traffic.

**IA Controls:** DCBP-1 Security Design, ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

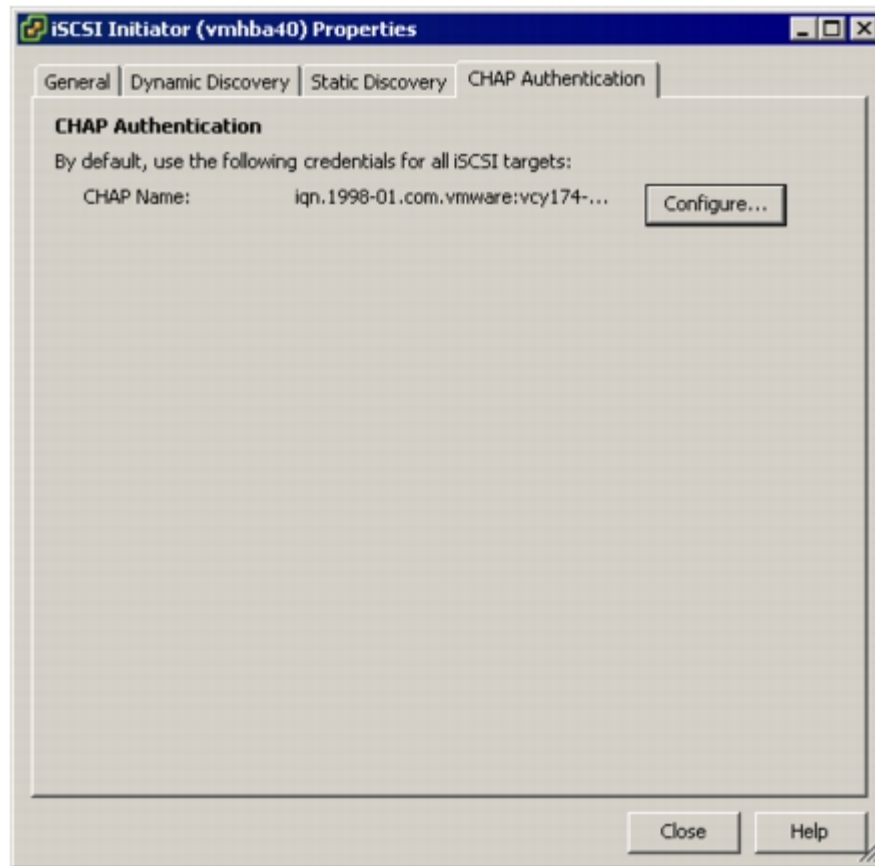
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** iSCSI connections are able to be configured with Challenge Handshake Authentication Protocol (CHAP) authentication and IP security (IPSec) encryption. “ESX Server only supports one-way CHAP authentication for iSCSI. It does not support Kerberos, Secure Remote Protocol (SRP), IPSec, or public key authentication methods for iSCSI authentication.” For both software and hardware iSCSI initiators, configuring CHAP for iSCSI connections will ensure proper authentication. “After the iSCSI initiator establishes the initial connection with the target, CHAP verifies the identity of the initiator and checks a CHAP secret that the initiator and the target share. This can be repeated periodically during the iSCSI session.”

**Computing Check:** To check the authentication method, perform the following within VirtualCenter:

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.
2. Click the Configuration tab and click Storage Adapters.
3. Select the iSCSI adapter to check and click the Properties to open the iSCSI Initiator Properties dialog box.
4. Click CHAP Authentication. If the CHAP Name shows a name, often the iSCSI initiator name, the iSCSI SAN is using CHAP authentication, and this is Not a Finding. See Figure below for CHAP authentication example.
5. If the CHAP Name shows Not Specified, then the iSCSI SAN is not using CHAP authentication, and this is a finding.



**Fix:** Enable CHAP authentication for iSCSI SAN connections.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0080:** iSCSI storage equipment is not configured with the latest patches and updates

**Vulnerability Key:** V0015790

**STIG ID:** ESX0080

**Vulnerability:** iSCSI storage equipment is not configured with the latest patches and updates.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator



**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The ESX Server does not open any ports to listen for network connections. This measure reduces the chances that an intruder can attack the ESX Server through spare ports and possibly compromise the server. However, iSCSI device vulnerabilities may exist even though the ESX Server is configured properly. If security vulnerabilities exist in the iSCSI device software, data located on the iSCSI device may be at risk. To mitigate this risk, system administrators will install all security patches provided by the storage equipment manufacturer and limit the devices connected to the iSCSI network.

**Computing Check:** Validating the iSCSI device software will require the assistance of the system administrator. The system administrator will have to give you the version number of the software and validate that the software is at the latest version. If the software is not at the latest version, then this is a finding.

**Fix:** Install the latest patches and updates to the iSCSI device.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0090:** iSCSI passwords are not in accordance with DoD policy

**Vulnerability Key:** V0015791

**STIG ID:** ESX0090

**Vulnerability:** iSCSI passwords are not in accordance with DoD policy.

**IA Controls:** IAIA-1 Individual Identification and Authentication, IAIA-2 Individual Identification and Authentication

**Categories:** 1.1 Passwords

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Storage administrators will protect storage configuration data from unauthorized users by using passwords that are in accordance with the policy in DoDI 8500.2

**Computing Check:** Work with the system administrator to determine compliance. Request the system administrator login to the iSCSI storage device and verify that the password is 14 characters. Review the complexity requirements are met by reviewing the configuration with the system administrator. The complexity requirements are one upper case letter, one lower case letter, one special character, and one number. If the password does not meet the requirements, then this is a finding.

**Fix:** Configure all iSCSI passwords according to DoD policy.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0100:** Static discoveries are not configured for hardware iSCSI initiators

**Vulnerability Key:** V0015792

**STIG ID:** ESX0100

**Vulnerability:** Static discoveries are not configured for hardware iSCSI initiators.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** ESX Server uses two types of methods to determine what storage resources are available for access by the iSCSI initiators on the network. These methods are dynamic discovery and static discovery. With dynamic discovery, the initiator discovers iSCSI targets by sending a SendTargets request to a specified target address. The target device responds by forwarding a list of additional targets that the initiator is allowed to access. The static discovery method uses the SendTargets request and returned is the list of available targets. Targets are listed on the static discovery list. This list may be modified by the storage administrator by adding or removing targets. The static discovery method is available only with the hardware-initiated storage. Hardware iSCSI initiators will use static discovery since it

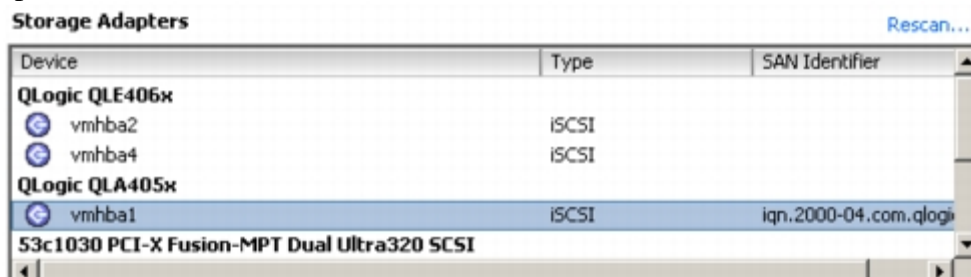
reduces the likelihood of connecting to some rogue target since all the targets are defined in the static list.

### Computing Check:

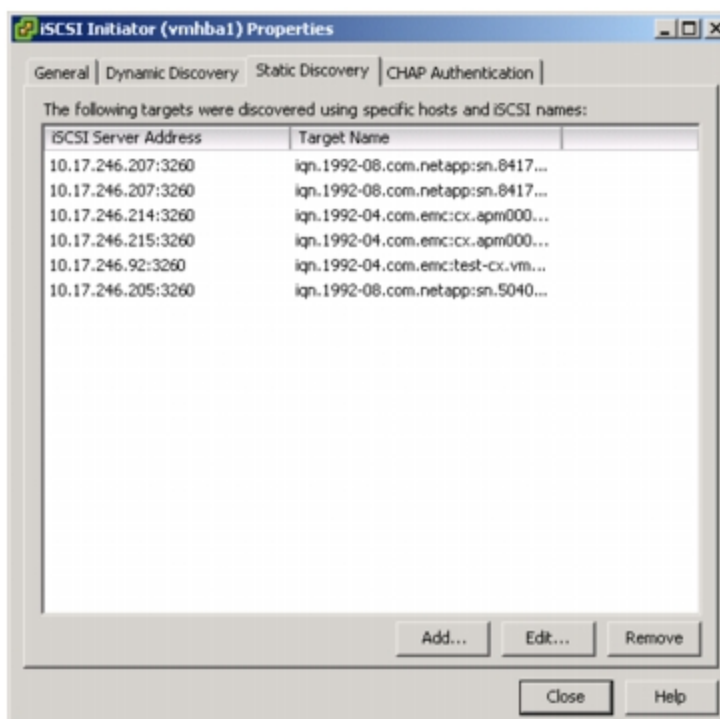
This check only applies if hardware iSCSI initiators are used. If they are used, then perform the following steps to verify static discovery is being used.

1. Log into VirtualCenter with the VI Client and select a ESX server from the inventory panel.
2. Click the Configuration tab and click Storage Adapters in the Hardware group.

The list of available adapters (initiators) appears. The iSCSI initiator appears in the list of storage adapters.



3. Under HBA, choose the initiator to review.
4. Click Properties, and then click the Static Discovery tab to verify that iSCSI targets are configured. If none are configured, then this is a finding.
5. Next verify that the dynamic discovery tab has no listings. If it does, then this is a finding.



**Fix:** Configure hardware initiators to use static discovery only.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0110:** USB drives load automatically when inserted into the ESX Server

**Vulnerability Key:** V0015793

**STIG ID:** ESX0110

**Vulnerability:** USB drives load automatically when inserted into the ESX Server host.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** External USB drives may be inserted into the ESX Server and be loaded automatically on the service console. The USB drive will still need to be mounted, but drivers are loaded to recognize the device. Malicious users may be able to run malicious code on the ESX Server and go undetected since the USB drive is external. Therefore, USB drives will not be loaded automatically within the ESX Server.

**Computing Check:** At the ESX Server service console terminal, type the following:

```
#cd /etc
```

```
#cat modules.conf
```

Verify that all "alias usb-controller" text is commented out with a pound sign (#).

Text should look similar to the following:

```
#alias usb-controller usb-uhci
```

```
#alias usb-controller1 usb-ohci
```

If not, then this is a finding.

**Fix:** Disable the external USB drive from loading automatically.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0120:** The ESX Server does not meet the minimum requirement of two network adapters

**Vulnerability Key:** V0015801

**STIG ID:** ESX0120

**Vulnerability:** The ESX Server does not meet the minimum requirement of two network adapters.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** A minimum of two physical network adapters is required in each physical server to enable networking for both the service console and the virtual machines. A minimum of two network adapters per ESX Server are required because the first network adapter discovered during the installation of the ESX Server is always dedicated to the service console by default. Up to 16 physical network adapters are supported per ESX Server. The ESX Server service console network adapter connects to the management user interface, SCP, SSH, and any other tool used to access the ESX Server's file system. The other physical network adapter will be dedicated to the virtual machines.

**Computing Check:** Go to the ESX Server service console, and type the following:

```
#esxcfg-nics -l
```

```
Vmnic0
```

```
Vmnic1
```

If you do not see vmnic0 and vmnic1 in the listing, then this is a finding. A minimum of two nics is required.

**Fix:** Configure the ESX Server with two network adapters.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0130:** The service console and virtual machines are not on dedicated VLANs or network segments

**Vulnerability Key:** V0015802

**STIG ID:** ESX0130

**Vulnerability:** The service console and virtual machines are not on dedicated VLANs or network segments.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

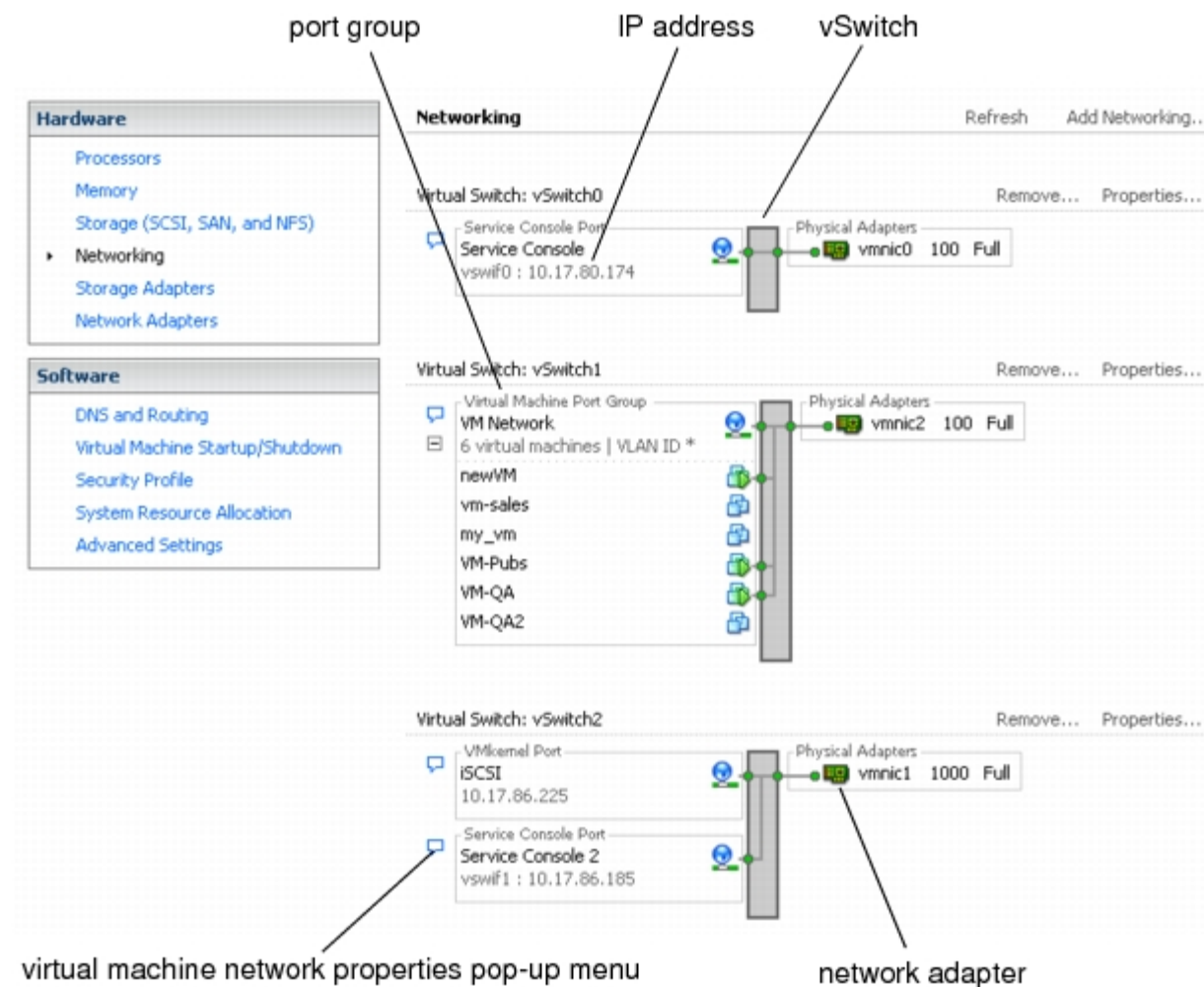
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machine traffic destined for a physical network should always be placed on a separate physical adapter from service console traffic. It is appropriate to use as many additional physical adapters as are necessary to support virtual machine networks. It may be sufficient to place the service console and virtual machine networks on separate VLANs connected to the same adapter, but connecting them to separate physical networks provides better isolation and more configuration control than is available using VLANs alone. The ESX Server VLAN implementation provides adequate network isolation, but it is possible that traffic could be misdirected due to improper configuration or security vulnerabilities in external networking hardware. It is safer to keep them physically separate.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel. The hardware configuration page for the server appears.
2. Click the Configuration tab, and click Networking.
3. Examine the virtual switches and their respective VLAN IDs. A separate VLAN ID should be configured for the service console and virtual machine traffic. If the virtual machines and service console are on the same VLAN ID, then this is a finding. See the figure below that demonstrates separate VLAN IDs.



**Fix:** Configure separate VLANs or network segments for the service console and virtual machine traffic.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0140:** Notify Switches feature is not enabled to allow for notifications to be sent to physical switches

**Vulnerability Key:** V0015803

**STIG ID:** ESX0140

**Vulnerability:** Notify Switches feature is not enabled to allow for notifications to be sent to physical switches.

## **IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

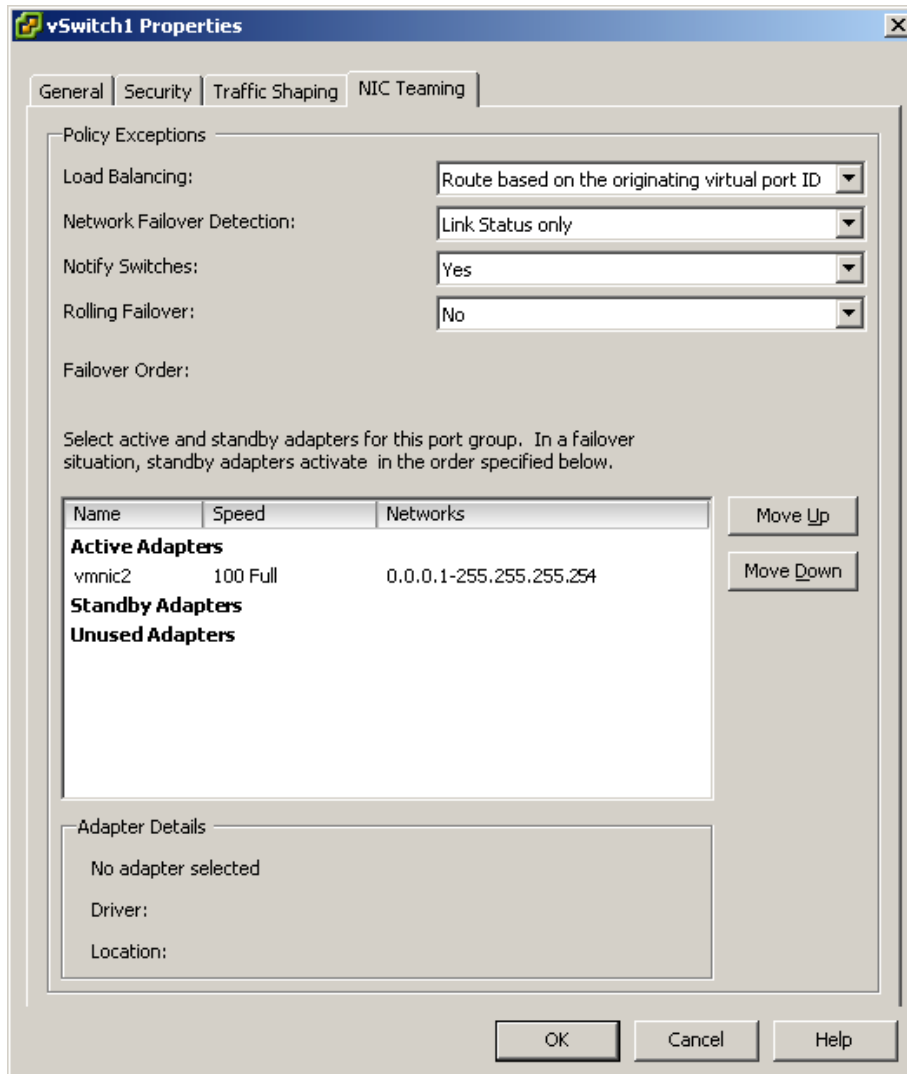
**Severity:** Category III

**Vulnerability Discussion:** One option in NIC Teaming is Notify Switches. Whenever a virtual NIC is connected to a virtual switch or whenever a virtual NIC's traffic would be routed over a different physical NIC due to a failover event, a notification is sent. This notification is sent out over the network to update the lookup tables on physical switches. Configuring this to 'Yes' sends out these notifications while providing the lowest latency of failover occurrences and migrations with VMotion.

### **Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel. The hardware configuration page for the server appears.
2. Click the Configuration tab, and click Networking.
3. Select a vSwitch and click Properties.
4. In the vSwitch Properties dialog box, click the Ports tab.
5. Select the vSwitch and click Edit.
6. Click the NIC Teaming tab.
7. Verify that Notify Switches is set to "Yes". If not, then this is a finding. See Figure below.





**Fix:** Enable Notify Switches feature to allow for notifications to be send to physical switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0150:** The ESX Server external physical switch ports are configured to VLAN 1

**Vulnerability Key:** V0015804

**STIG ID:** ESX0150

**Vulnerability:** The ESX Server external physical switch ports are configured to VLAN 1.

## IA Controls: ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Physical switches use the native VLAN for switch control and management protocol. Native VLAN frames are not tagged with any VLAN ID in many types of switches. The trunk ports implicitly treat all untagged frames as native VLAN frames. VLAN 1 is the default native VLAN ID for many commercial switches. However, in many enterprise networks, the native VLAN might be VLAN 1 or any number depending on the switch type. ESX Server does not support virtual switch port groups configured to VLAN 1. If the physical switch port that the ESX Server is connected to is configured with VLAN 1, the ESX Server will drop all packets. The ESX Server virtual switch port groups will be configured with any value between 2 and 4094. Utilizing VLAN 1 will cause a denial of service since the ESX Server drops this traffic.

**Computing Check:** Work with the network reviewer and system administrator to determine compliance. Go to the switch that connects the ESX Server to the network. Request a copy of switch configuration to verify the ports that the ESX Server plugs into are not configured to VLAN 1. Below is an example of disabling VLAN 1 and creating a VLAN that may be used for ESX Server traffic.

```
Interface VLAN1
```

```
no ip address
```

```
shutdown
```

```
interface VLAN 12
```

```
ip address 10.0.0.25 255.255.255.0
```

```
no shutdown
```

```
set interface sc0 10.0.0.25 255.255.255.0
```

**Fix:** Configure ESX Server external physical switches to something other than VLAN 1.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0160:** Permissions have been changed on the /usr/sbin/esxcfg-\* utilities

**Vulnerability Key:** V0015805

**STIG ID:** ESX0160

**Vulnerability:** Permissions have been changed on the /usr/sbin/esxcfg-\* utilities.

**IA Controls:** ECCD-1, ECCD-2 Changes to Data, ECAN-1 Access to Need to Know

**Categories:** 2.1 Object permissions

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Configuring virtual switches may be performed by using predefined ESX Server commands. These commands are located in the /usr/bin of the file system hierarchy. Since these commands can create, disable, and modify existing configurations, they will be restricted to the root user only. If other users were able to access these commands, inadvertent changes could potentially disable a virtual network.

**Computing Check:** Logon to the ESX Server service console, and perform the following to review the permissions on the esxcfg-\* utilities.

```
#cd /usr/sbin
```

```
#ls -l | grep esxcfg | less
```

All permissions here should be 500 except for esxcfg-auth which should be 544. If they are not 500, then this is a finding.

```
#ls -l | grep esxcfg-auth
```

Permissions on the esxcfg-auth should be 544, if not then this is a finding.

```
#ls -l | grep esxupdate
```

Permissions on the esxupdate should be 544, if not then this is a finding.

**Fix:** Do not modify the /usr/sbin/esxcfg-\* and esxupdate utilities.

Comments:
-----------

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0170:** Virtual machines are connected to public virtual switches and are not documented

**Vulnerability Key:** V0015806

**STIG ID:** ESX0170

**Vulnerability:** Virtual machines are connected to public virtual switches and are not documented.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 2.2 Least Privilege

**Responsibility:** Information Assurance Officer / System Administrator

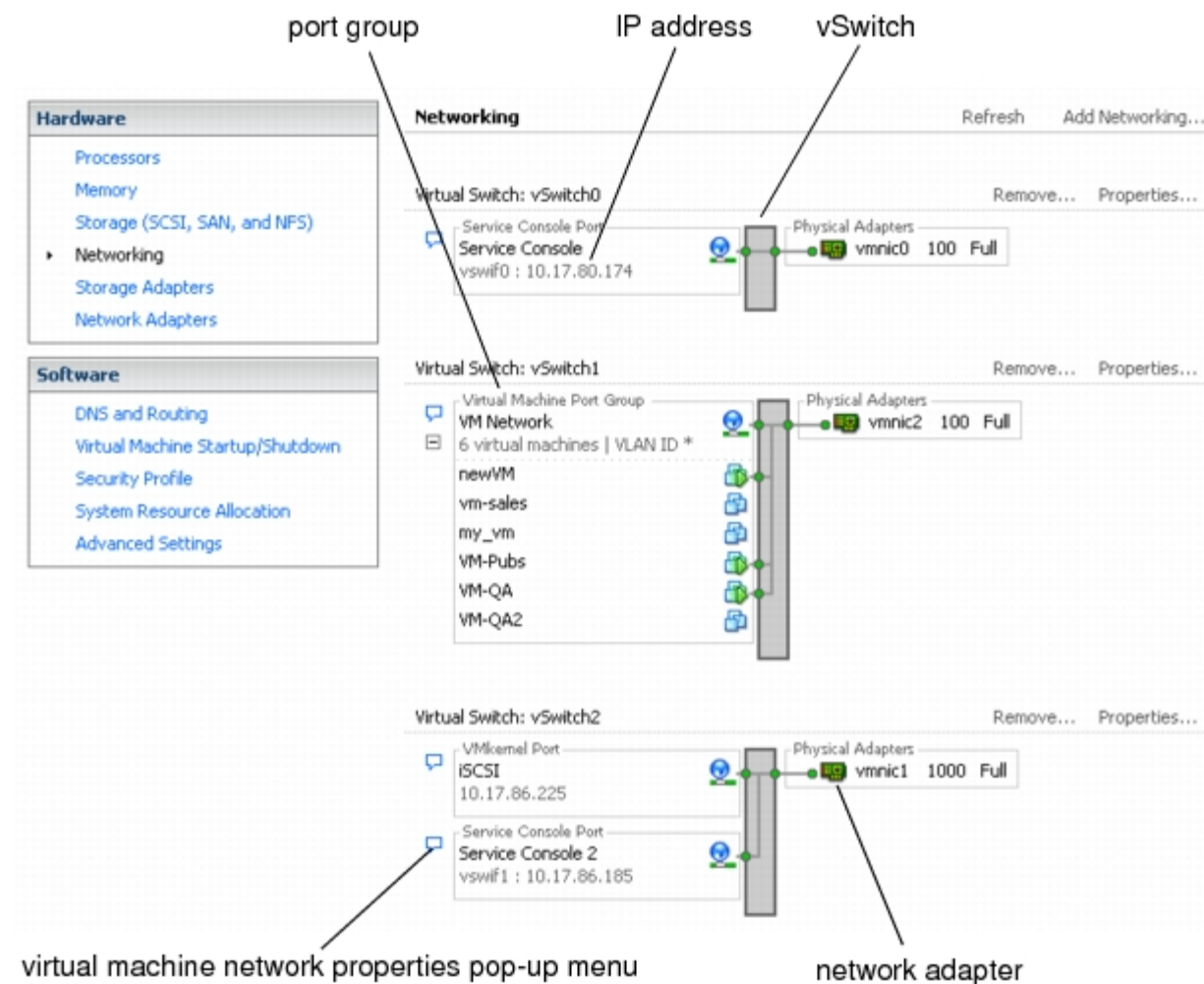
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Public virtual switches are bound to physical NICs providing virtual machines connectivity to the physical network, whereas connecting physical servers to the LAN usually requires a cable. Virtual network configuration is much easier since once a virtual machine is attached to a virtual switch, these machines are able to send and receive packets. Care must be taken as to which virtual machines have access to the physical network through the public virtual switches. The master configuration file for virtual switches is the esx.conf file.

**Computing Check:**

1. Request the documentation for all virtual machines connected to public virtual switches. If no documentation exists or the documentation is not accurate, then this is a finding.
2. Log into VirtualCenter with the VI Client, and select the ESX server from the inventory panel.  
The hardware configuration page for the server appears.
3. Click the Configuration tab, and click Networking.
4. Review all virtual switches that have virtual machines connected to them that may access the external network. In the diagram below, vSwitch1 should be reviewed to ensure the virtual machines connected to it are documented with the IAO/SA. Compare the actual configuration of the documentation and verify no discrepancies exist. If so, then this is a finding.



**Fix:** Document all virtual machines that need access to public virtual switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0180:** Virtual switch port group is configured to VLAN 1

**Vulnerability Key:** V0015807

**STIG ID:** ESX0180

**Vulnerability:** Virtual switch port group is configured to VLAN 1.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

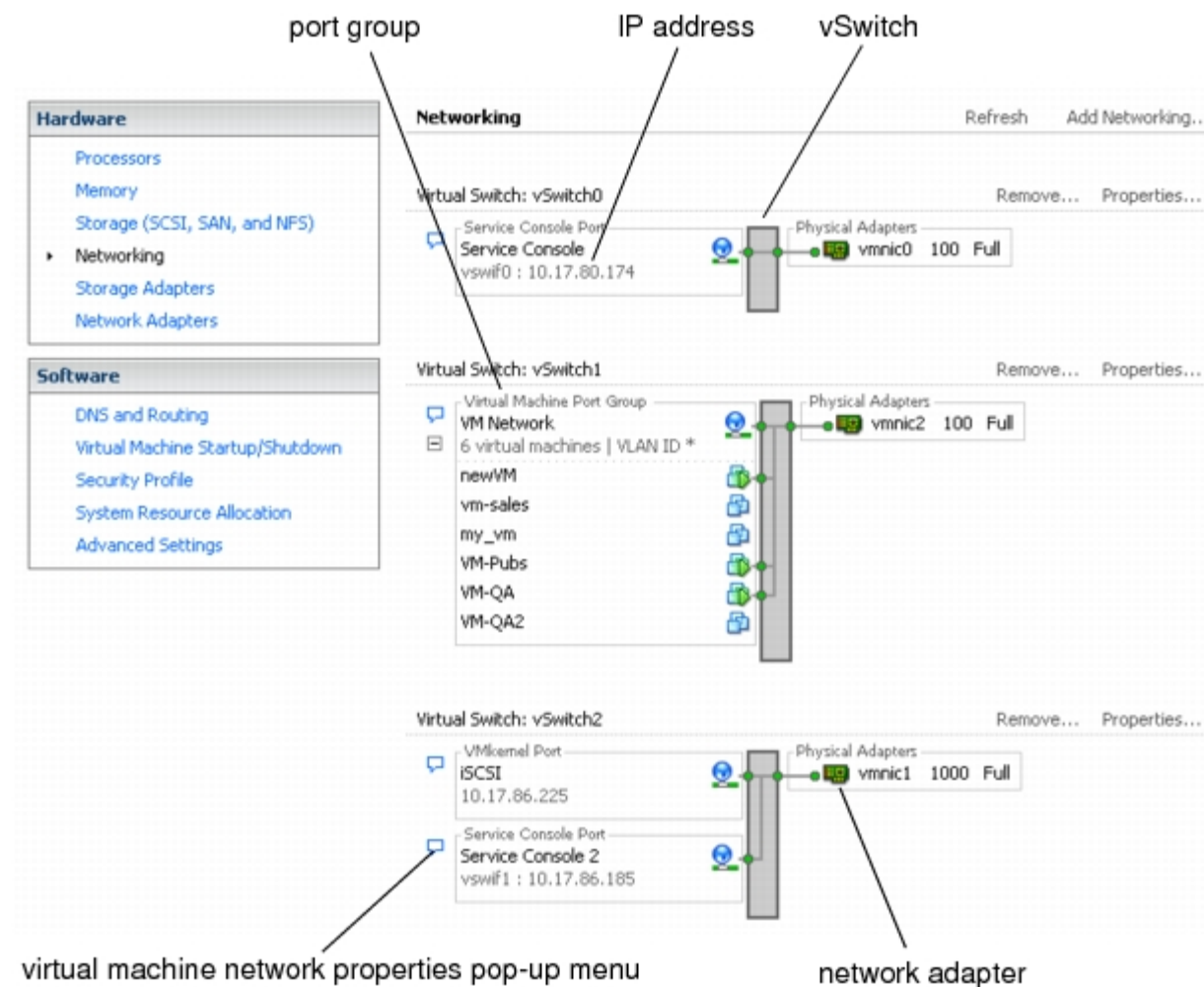
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The VLAN ID restricts port group traffic to a logical Ethernet segment within the physical network. Port groups may have a VLAN ID of 0 to 4095. VLAN ID values of 1 to 4094 place the virtual switch in VST mode. However VLAN 1 will not be enabled for port groups since ESX Server does not support virtual switch port groups configured to VLAN 1. VLAN 1001 through 1024 are Cisco reserved VLANs. VLANs 1, 1001 to 1024, and 4095 will be not be used for virtual switch port groups since they may cause unexpected operation.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.
2. Click the Configuration tab and click Networking.  
Virtual switches are presented in a layout that shows an overview and details.
3. On the right side of the window, click Properties for a network.
4. Click the Ports tab.
5. In the Properties dialog box for the port group, click the General tab to check the VLAN ID. If the VLAN ID is set to 1, then this is a finding.



**Fix:** Do not configure virtual switch VLAN IDs to be VLAN 1, 1001-1024, and 4095.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0190:** Virtual switch port group is configured to VLAN 1001 to 1024

**Vulnerability Key:** V0015808

**STIG ID:** ESX0190

**Vulnerability:** Virtual switch port group is configured to VLAN 1001 to 1024.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

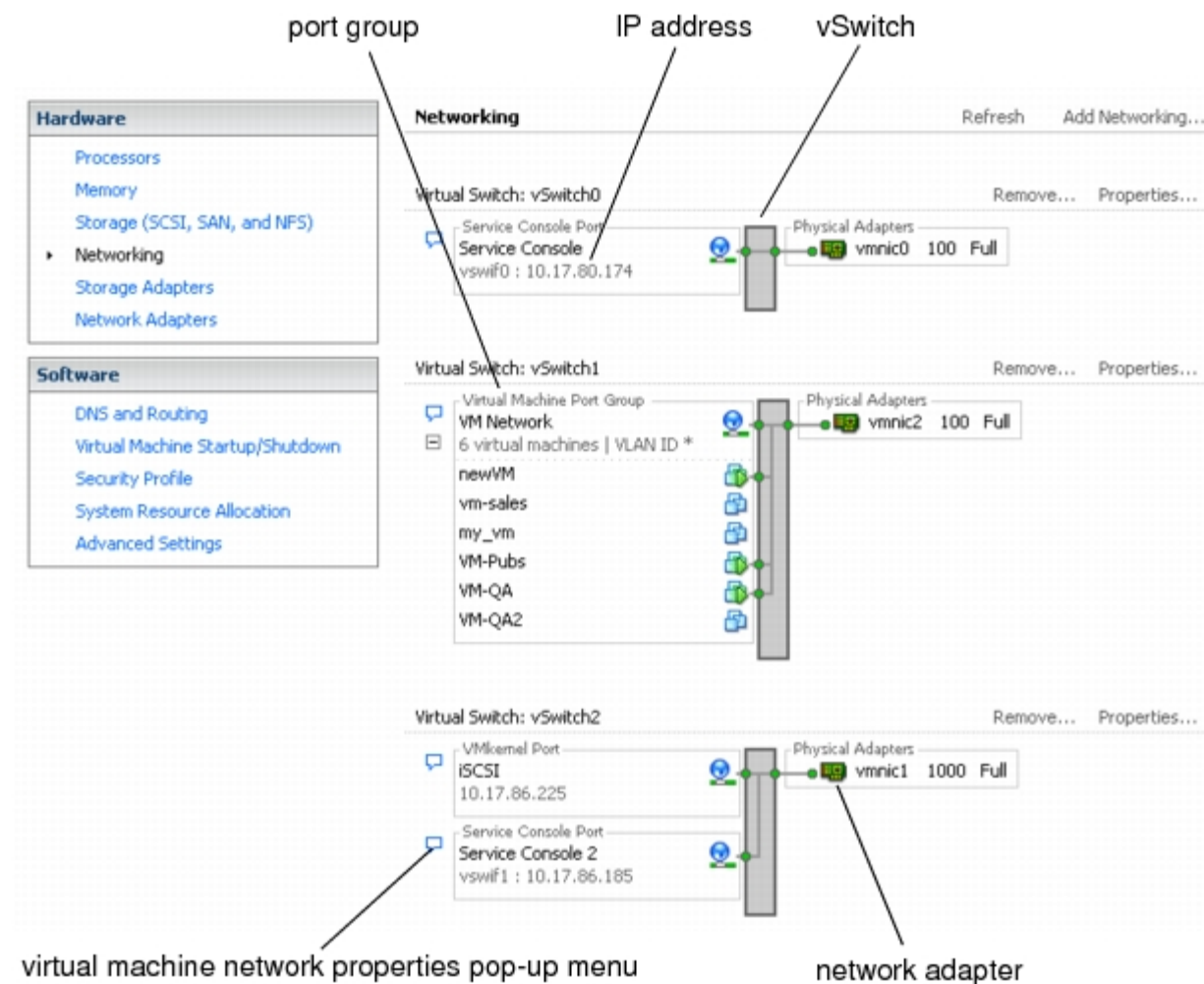
**Severity:** Category II

**Vulnerability Discussion:** The VLAN ID restricts port group traffic to a logical Ethernet segment within the physical network. Port groups may have a VLAN ID of 0 to 4095. VLAN ID values of 1 to 4094 place the virtual switch in VST mode. However VLAN 1 will not be enabled for port groups since ESX Server does not support virtual switch port groups configured to VLAN 1. VLAN 1001 through 1024 are Cisco reserved VLANs. VLANs 1, 1001 to 1024, and 4095 will be not be used for virtual switch port groups since they may cause unexpected operation.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.
2. Click the Configuration tab and click Networking.  
Virtual switches are presented in a layout that shows an overview and details.
3. On the right side of the window, click Properties for a network.
4. Click the Ports tab.
5. In the Properties dialog box for the port group, click the General tab to check the VLAN ID. If the VLAN ID is set to 1001 to 1024, then this is a finding.





**Fix:** Do not configure virtual switch VLAN IDs s to be VLAN 1, 1001-1024, and 4095.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0200:** Virtual switch port group is configured to VLAN 4095

**Vulnerability Key:** V0015809

**STIG ID:** ESX0200

**Vulnerability:** Virtual switch port group is configured to VLAN 4095.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

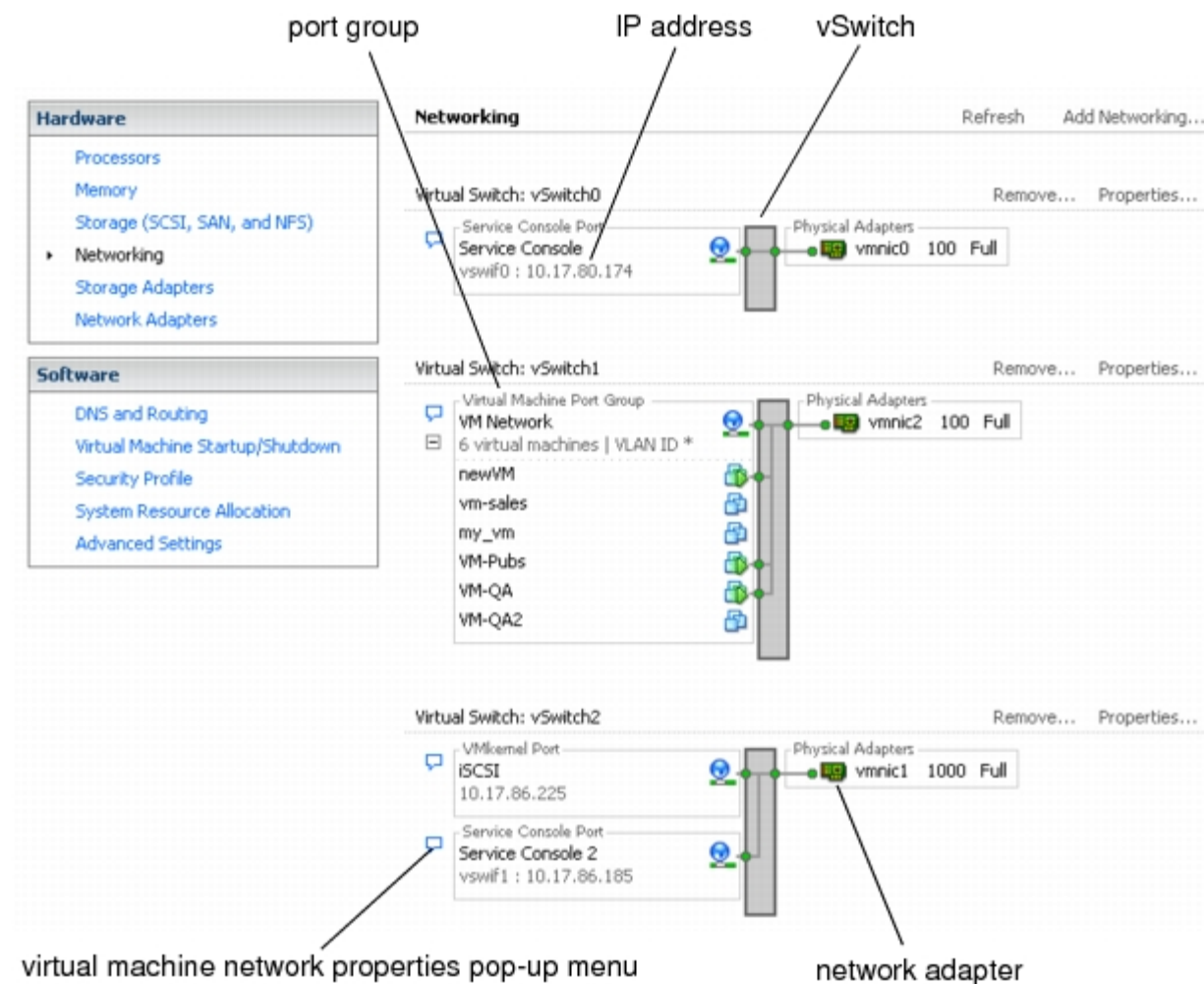
**Severity:** Category II

**Vulnerability Discussion:** The VLAN ID restricts port group traffic to a logical Ethernet segment within the physical network. Port groups may have a VLAN ID of 0 to 4095. VLAN IDs that have VLAN ID 4095 are able reach other port groups located on other VLANs. Basically, VLAN ID 4095 specifies that the port group should use trunk mode or VGT mode, which allows the guest operating system to manage its own VLAN tags. Guest operating systems typically do not manage their VLAN membership on networks. VLAN 1001 through 1024 are Cisco reserved VLANs. VLANs 1, 1001 to 1024, and 4095 will be not be used for virtual switch port groups since they may cause unexpected operation.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.
2. Click the Configuration tab and click Networking.  
Virtual switches are presented in a layout that shows an overview and details.
3. On the right side of the window, click Properties for a network.
4. Click the Ports tab.
5. In the Properties dialog box for the port group, click the General tab to check the VLAN ID. If the VLAN ID is set to 4095, then this is a finding.

**Caveat:** This check is Not Applicable if the number of VLANs needed for the virtual machine exceeds 4 VLANs, and it is documented with the IAO/SA.



**Fix:** Do not configure virtual switch VLAN IDs to be VLAN 1, 1001-1024, and 4095.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0210:** Port groups are not configured with a network label

**Vulnerability Key:** V0015810

**STIG ID:** ESX0210

**Vulnerability:** Port groups are not configured with a network label.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 11.1 Marking

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

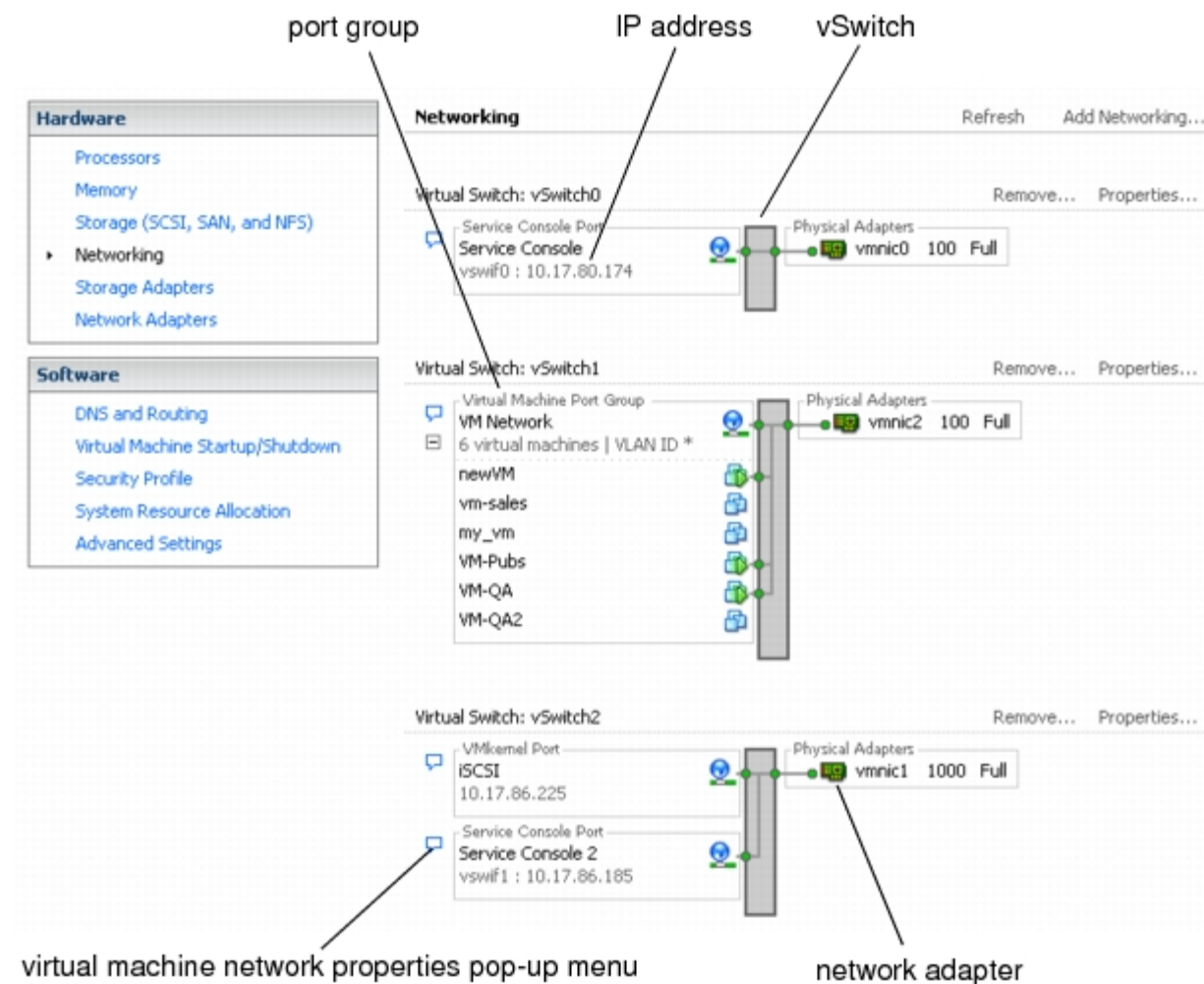
**Vulnerability Discussion:** Port Groups define how virtual machine connections are made through the virtual switch. Port groups may be configured with bandwidth limitations and VLAN tagging policies for each member port. Multiple ports may be aggregated under port groups to provide a local point for virtual machines to connect to a network. The maximum number of port groups that may be configured on a virtual switch is 512. Each port group is identified by a network label and a VLAN ID. Network labels identify the port groups with a name. These names are important since they serve as a functional descriptor for the port group. Without these descriptions, identifying port groups and their functions becomes difficult as the network becomes more complex.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.
2. Click the Configuration tab and click Networking.

Virtual switches are presented in a layout that shows an overview and details.

3. On the right side of the window, click Properties for a network.
4. Click the Ports tab.
5. In the Properties dialog box for the port group, click the General tab to check the Network Label. If no Network Label is configured, then this is a finding. In the figure below, the network label is service console for vSwitch0.



**Fix:** Configure a network label for all virtual switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0220:** Unused port groups have not been removed

**Vulnerability Key:** V0015811

**STIG ID:** ESX0220

**Vulnerability:** Unused port groups have not been removed.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

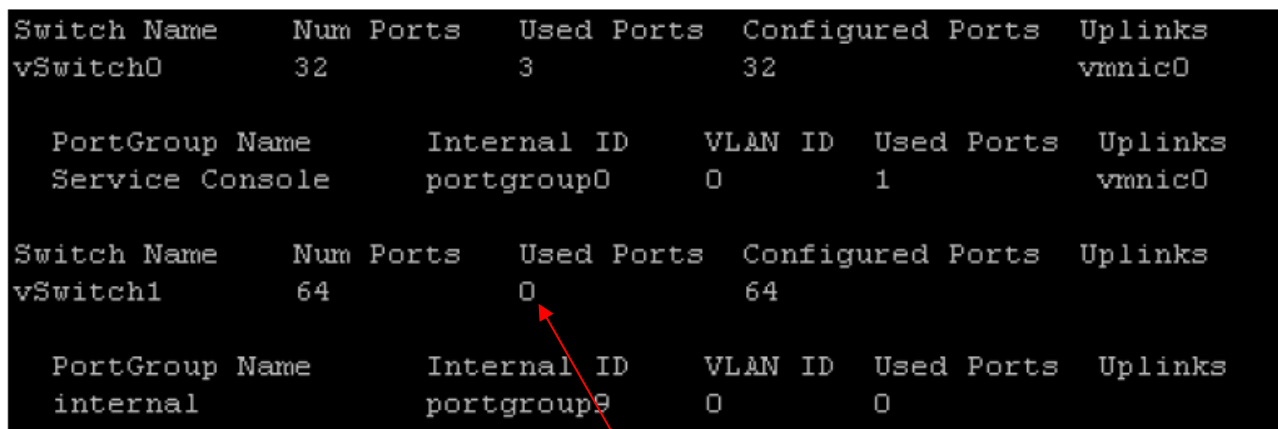
**Severity:** Category II

**Vulnerability Discussion:** Port groups define how virtual machine connections are made through the virtual switch. Port groups may be configured with bandwidth limitations and VLAN tagging policies for each member port. Multiple ports may be aggregated under port groups to provide a local point for virtual machines to connect to a network. The maximum number of port groups that may be configured on a virtual switch is 512. Each port group is identified by a network label and a VLAN ID. As with any physical switch, all unused virtual switch port groups will be removed if not in use. Physical switches place these unused ports in unused VLANs and shutdown the port. For the ESX Server, these port groups must be removed to ensure that they are not used by mistake.

**Computing Check:**

Work with the system administrator to gain access to the ESX Server service console to perform the following command.

#esxcfg-vswitch -l



Switch Name	Num Ports	Used Ports	Configured Ports	Uplinks
vSwitch0	32	3	32	vmnic0
PortGroup Name	Internal ID	VLAN ID	Used Ports	Uplinks
Service Console	portgroup0	0	1	vmnic0
Switch Name	Num Ports	Used Ports	Configured Ports	Uplinks
vSwitch1	64	0	64	
PortGroup Name	Internal ID	VLAN ID	Used Ports	Uplinks
internal	portgroup9	0	0	

Used ports equals 0

If the 'Used Ports' has the number 0, then this is a finding.

**Caveat:** VMotion, HA, and DRS virtual switches may have unused port groups. This check is not applicable to these switches. Also, if VMotion is configured for a virtual machine(s), then when VMotion occurs, a duplicate virtual switch will be configured so the virtual machine can run once the migration is complete. These virtual switches will have 0 used ports until it is VMotioned to the ESX Server host. Therefore, virtual switches in this scenario are not

applicable to this check. These virtual switches must be available for proper VMotion, HA, and DRS purposes.

**Fix:** Remove all unused port groups from virtual switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0230:** Virtual switches are not labeled

**Vulnerability Key:** V0015812

**STIG ID:** ESX0230

**Vulnerability:** Virtual switches are not labeled.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

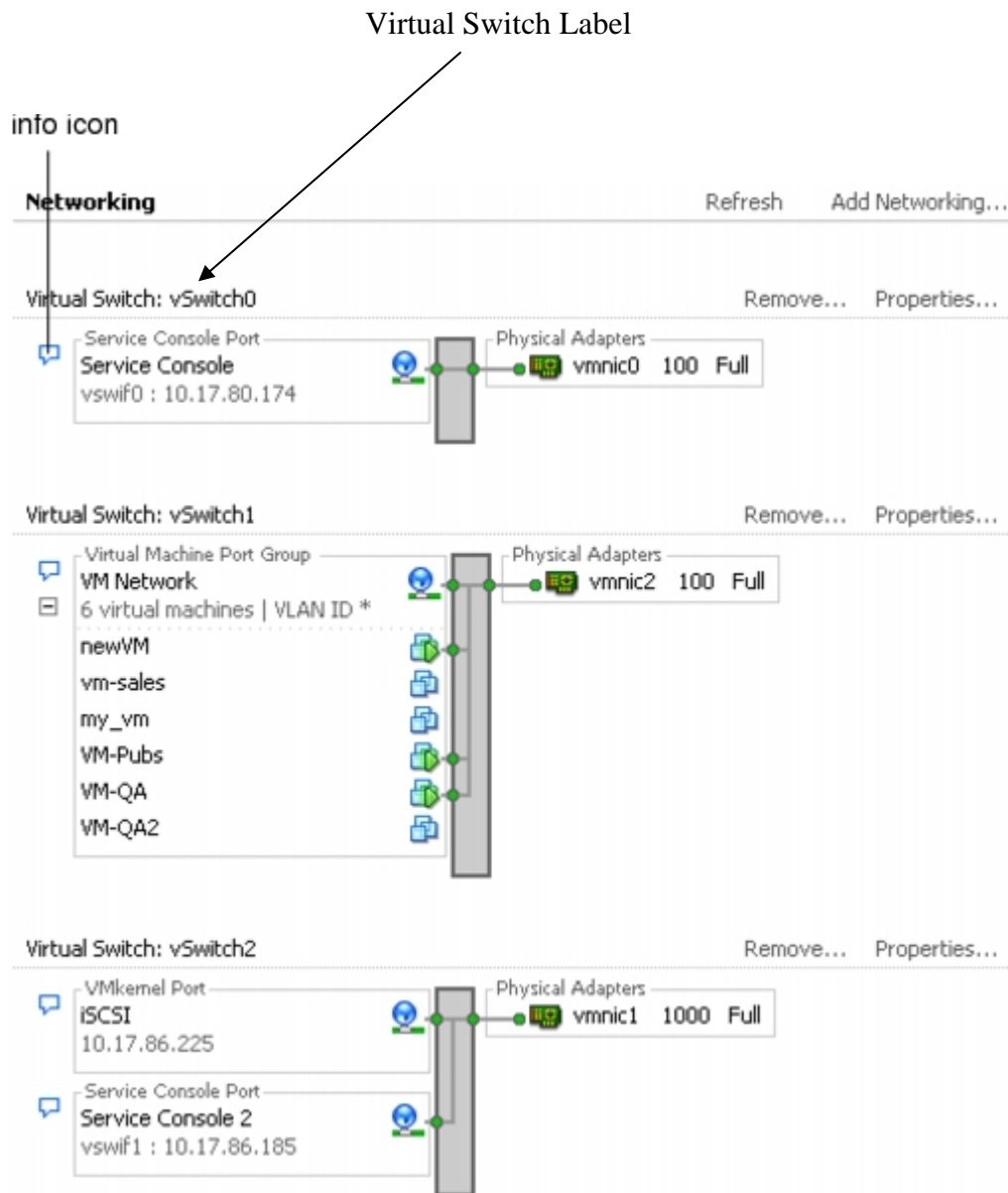
**Severity:** Category II

**Vulnerability Discussion:** Virtual switches within the ESX Server require a field for the name of the switch. This label is important since it serves as a functional descriptor for the switch, just as physical switches require a hostname. Labeling virtual switches will indicate the function or the IP subnet of the virtual switch. For instance, labeling the virtual switch as “internal” or some variation will indicate that the virtual switch is only for internal networking between virtual machines private virtual switch with no physical network adapters bound to it.

**Computing Check:**

To check to see if virtual switches have labels, perform the following within VirtualCenter:

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.  
The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.  
The figure below should appear. Ensure that all virtual switches have a label. If they do not, then this is a finding.



**Fix:** Label all virtual switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--



**ESX0240:** Virtual switch labels begin with a number

**Vulnerability Key:** V0015813

**STIG ID:** ESX0240

**Vulnerability:** Virtual switch labels begin with a number.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

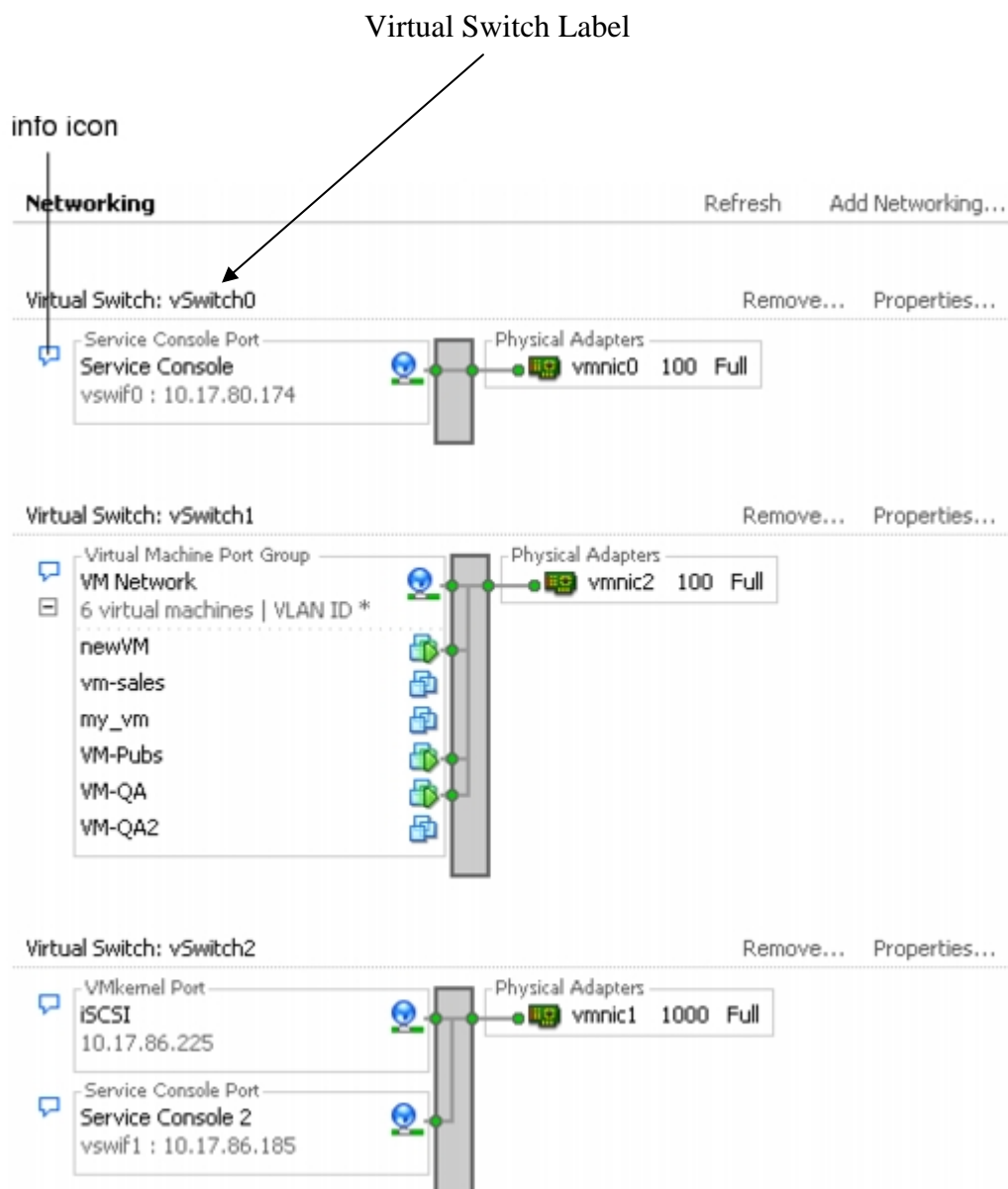
**Severity:** Category II

**Vulnerability Discussion:** Virtual switches within the ESX Server require a field for the name of the switch. This label is important since it serves as a functional descriptor for the switch. Labeling the virtual switches will not contain the first character as a number, since there have been known issues in the past that have caused erratic behavior. This has been especially true when renaming or removing the virtual switch. Labeling virtual switches will indicate the function or the IP subnet of the virtual switch. For instance, labeling the virtual switch as “internal” or some variation will indicate that the switch is only for internal networking between virtual machines private virtual switch with no physical network adapters bound to it.

**Computing Check:** To check to see if virtual switches have labels, perform the following within VirtualCenter:

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.  
The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.

The figure below should appear. Ensure that all virtual switches have a label that does not start with a number. If the virtual switches begin with a number, then this is a finding.



**Fix:** Do not begin virtual switch labels with a number.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0250:** The MAC address change 'Policy' is set to Accept for virtual switches

**Vulnerability Key:** V0015815

**STIG ID:** ESX0250

**Vulnerability:** The MAC address change 'Policy' is set to Accept for virtual switches.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

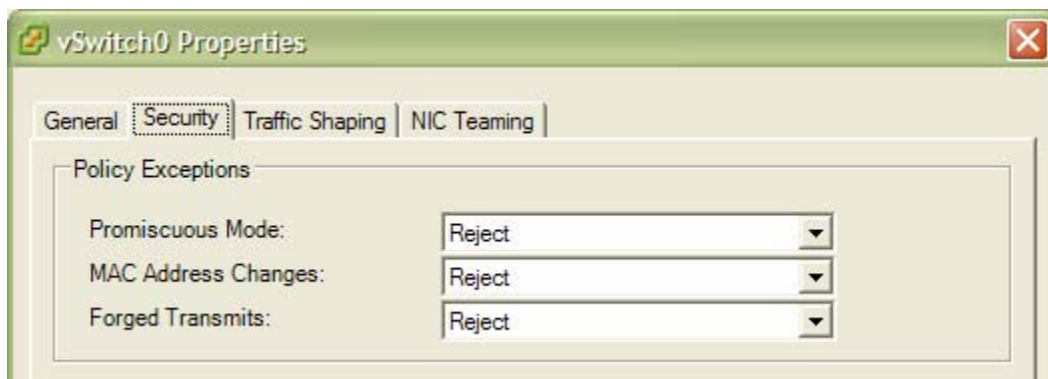
**Severity:** Category I

**Vulnerability Discussion:** Each virtual NIC in a virtual machine has an initial MAC address assigned when the virtual adapter is created. Each virtual adapter also has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. A virtual adapter's effective MAC address and initial MAC address are the same when they are initially created. However, the virtual machine's operating system may alter the effective MAC address to another value at any time. If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network. System administrators can use virtual switch security profiles on ESX Server hosts to protect against this type of attack by setting two options on virtual switches. These options are MAC Address Changes and Forged Transmits.

MAC address changes are set to accept by default meaning that the virtual switch accepts requests to change the effective MAC address. The MAC Address Changes option setting affects traffic received by a virtual machine. To protect against MAC impersonation this option will be set to reject, ensuring the virtual switch does not honor requests to change the effective MAC address to anything other than the initial MAC address. Setting this to reject disables the port that the virtual network adapter used to send the request. Therefore, the virtual network adapter does not receive any more frames until it configures the effective MAC address to match the initial MAC address. The guest operating system will not detect that the MAC address change has not been honored.

### Computing Check:

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.  
The hardware configuration page for the server appears.
2. Click the Configuration tab, and click Networking.
3. Click Properties for the virtual switch whose layer 2 policy you want to review.
4. In the Properties dialog box for the virtual switch, click the Ports tab.
5. Select the virtual switch item and click Edit.
6. In the Properties dialog box for the virtual switch, click the Security tab.
7. Verify the MAC Address Changes is set to Reject. If it is not, then this is a finding.



**Caveat:** This is not applicable for legacy applications, clustered environments, and licensing issues if documented and approved by the IAO/SA.

**Fix:** Configure the MAC Address Changes 'Policy' to Reject.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0260:** Forged Transmits are set to Accept for on virtual switches

**Vulnerability Key:** V0015617

**STIG ID:** ESX0260

**Vulnerability:** Forged Transmits are set to Accept on virtual switches.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

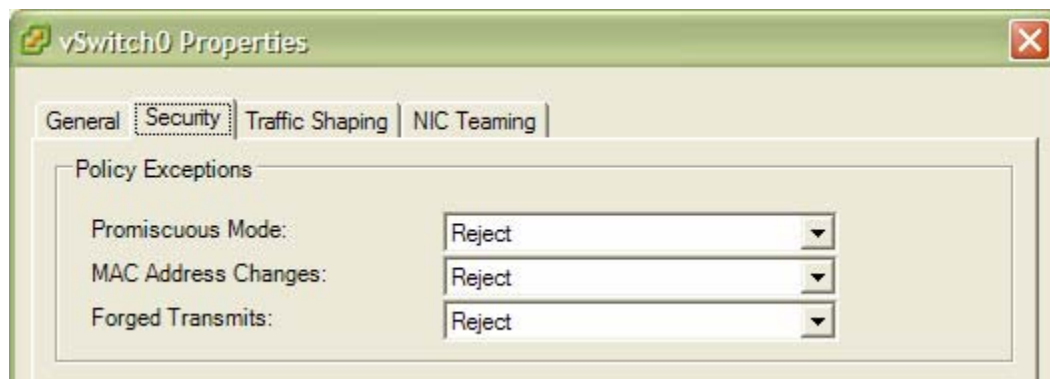
**Severity:** Category I

**Vulnerability Discussion:** Each virtual NIC in a virtual machine has an initial MAC address assigned when the virtual adapter is created. Each virtual adapter also has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. A virtual adapter's effective MAC address and initial MAC address are the same when they are initially created. However, the virtual machine's operating system may alter the effective MAC address to another value at any time. If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network. SAs can use virtual switch security profiles on ESX Server hosts to protect against this type of attack by setting two options on virtual switches. These options are MAC Address Changes and Forged Transmits.

Forged transmissions are set to accept by default. This means the virtual switch does not compare the source and effective MAC addresses. The Forged Transmits option setting affects traffic transmitted from a virtual machine. If this option is set to reject, the virtual switch compares the source MAC address being transmitted by the operating system with the effective MAC address for its virtual network adapter to see if they are the same. If the MAC addresses are different, the virtual switch drops the frame. The guest operating system will not detect that its virtual network adapter cannot send packets using the different MAC address. To protect against MAC address impersonation, all virtual switches will have forged transmissions set to reject.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel. The hardware configuration page for the server appears.
2. Click the Configuration tab, and click Networking.
3. Click Properties for the virtual switch whose layer 2 policy you want to review.
4. In the Properties dialog box for the virtual switch, click the Ports tab.
5. Select the virtual switch item and click Edit.
6. In the Properties dialog box for the virtual switch, click the Security tab.
7. Verify the Forged Transmits is set to Reject. If it is not, then this is a finding.



**Fix:** Configure the Forged Transmits 'Policy' to Reject.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0270:** Promiscuous Mode is set to Accept on virtual switches

**Vulnerability Key:** V0015818

**STIG ID:** ESX0270

**Vulnerability:** Promiscuous Mode is set to Accept on virtual switches.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category I

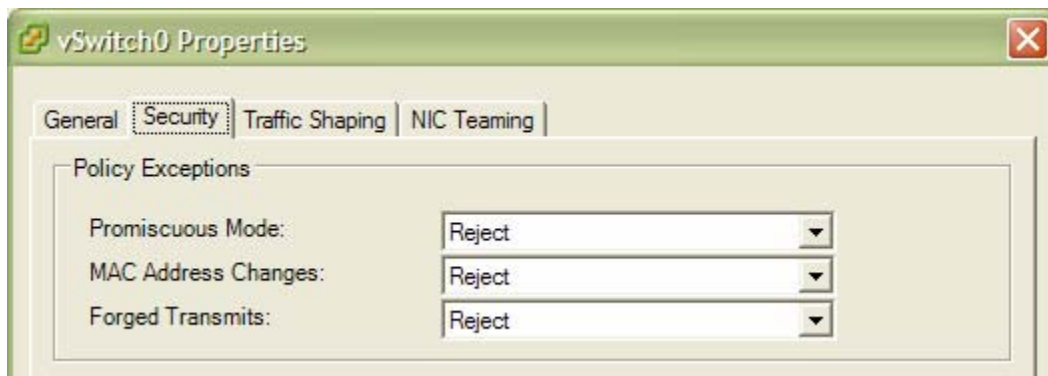
**Vulnerability Discussion:** ESX Server has the ability to run virtual and physical network adapters in promiscuous mode. Promiscuous mode may be enabled on public and private virtual switches. When promiscuous mode is enabled for a public virtual switch, all virtual machines connected to the public virtual switch have the potential of reading all packets sent across that network, from other virtual machines and any physical machines or other network devices. When promiscuous mode is enabled for a private virtual switch, all virtual machines connected to the private virtual switch have the potential of reading all packets across that network, meaning only

the virtual machines connected to that private virtual switch. By default, promiscuous mode is set to Reject, meaning that the virtual network adapter cannot operate in Promiscuous mode.

Promiscuous mode will be disabled on the ESX Server virtual switches since confidential data may be revealed while in this mode. Promiscuous mode is disabled by default on the ESX Server; however there might be a legitimate reason to enable it for debugging, monitoring, or troubleshooting reasons. To enable promiscuous mode for a virtual switch, a value is inserted into a special virtual file in the /proc file system.

### Computing Check:

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel. The hardware configuration page for the server appears.
2. Click the Configuration tab, and click Networking.
3. Click Properties for the virtual switch whose layer 2 policy you want to review.
4. In the Properties dialog box for the virtual switch, click the Ports tab.
5. Select the virtual switch item and click Edit.
6. In the Properties dialog box for the virtual switch, click the Security tab.
7. Verify the Promiscuous Mode is set to Reject. If it is not, then this is a finding.



**Note:** If promiscuous mode is turned on for troubleshooting purposes, then it must be documented and approved with the IAO/SA.

**Fix:** Configure the Promiscuous Mode 'Policy' to Reject.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0280:** Promiscuous mode is enabled for virtual switches during the ESX Server boot process

**Vulnerability Key:** V0015819

**STIG ID:** ESX0280

**Vulnerability:** Promiscuous mode is enabled for virtual switches during the ESX Server boot process.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 14.3 Network Device Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category I

**Vulnerability Discussion:** ESX Server has the ability to run virtual and physical network adapters in promiscuous mode. Promiscuous mode may be enabled on public and private virtual switches. When promiscuous mode is enabled for a public virtual switch, all virtual machines connected to the public virtual switch have the potential of reading all packets sent across that network, from other virtual machines and any physical machines or other network devices. When promiscuous mode is enabled for a private virtual switch, all virtual machines connected to the private virtual switch have the potential of reading all packets across that network, meaning only the virtual machines connected to that private virtual switch. By default, promiscuous mode is set to Reject, meaning that the virtual network adapter cannot operate in Promiscuous mode.

Promiscuous mode will be disabled on the ESX Server virtual switches since confidential data may be revealed while in this mode. Promiscuous mode is disabled by default on the ESX Server; however there might be a legitimate reason to enable it for debugging, monitoring, or troubleshooting reasons. To enable promiscuous mode for a virtual switch, a value is inserted into a special virtual file in the /proc file system. After a reboot of the ESX Server, promiscuous mode will be disabled again since the value is in the /proc directory. One way to ensure promiscuous mode is enabled indefinitely is to add a command to the /etc/rc.local boot script in the service console.

### **Computing Check:**

On the ESX service console, perform the following:

```
# less /etc/rc.local
#!/bin/sh
#
# This script will be executed *after* all other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
```



Touch /var/lock/subsys/local

If you see something similar to the following then this is a finding:

```
echo "PromiscuousAllowed yes" > /proc/vmware/net/vmnic0/config
```

**Note:** If promiscuous mode is turned on for troubleshooting purposes, then it must be documented and approved with the IAO/SA.

**Fix:** Disable promiscuous mode during the ESX Server boot process.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0290:** External physical switch ports configured for EST mode are configured with spanning-tree enabled

**Vulnerability Key:** V0015820

**STIG ID:** ESX0290

**Vulnerability:** External physical switch ports configured for EST mode are configured with spanning-tree enabled.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** EST mode has a one-to-one relationship, the number of VLANs supported on the ESX Server system is limited to the number of physical network adapter ports assigned to the VMkernel. EST is enabled when the port group's VLAN ID is set to 0 or left blank. Due to the integration of the ESX Server into the physical network, the physical network adapters will need to have spanning-tree disabled or portfast configured for external switches, since VMware virtual switches do not support STP. If these are not set, potential performance

and connectivity issues could arise. Virtual switch uplinks do not create loops within the physical switch network.

### Computing Check:

Request a copy of the external switch configuration that the ESX Server is connected to. Work with the network reviewer and system administrator to review the configuration to ensure that either spanning-tree is disabled for those ports or spanning-tree is configured to portfast. If either one of these conditions is not configured, then this is a finding.

Spanning-tree portfast configuration should look similar to the following if using the Cisco IOS:

```
Switch# show running-config interface <gigabit or fastethernet> <module/port number>
```

```
Interface gigabit 5/1
```

```
No ip address
```

```
Switchport
```

```
Switchport access vlan <number>
```

```
Switchport mode access
```

**Spanning-tree portfast**

```
End
```

```
Switch#
```

Spanning-tree disabled should look similar to the following if using Cisco IOS:

```
Switch# show running config
```

```
....
```

**No spanning-tree vlan <number>**

```
....
```

Should see the vlan number in the no spanning-tree vlan command.

**Fix:** Disable spanning-tree or configure spanning-tree to portfast for the external switch ports.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0300:** The non-negotiate option is not configured for trunk links between external physical switches and virtual switches in VST mode

**Vulnerability Key:** V0015821

**STIG ID:** ESX0300

**Vulnerability:** The non-negotiate option is not configured for trunk links between external physical switches and virtual switches in VST mode.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** In order to communicate with virtual switches in VST mode, external switch ports must be configured as trunk ports. VST mode does not support Dynamic Trunking Protocol (DTP), so the trunk must be static and unconditional. The auto or desirable physical switch settings do not work with the ESX Server because the physical switch expects the ESX Server to communicate using DTP. The non-negotiate and on options enable VLAN trunking on the physical switch unconditionally and create a VLAN trunk link between the ESX Server and the physical switch. The difference between non-negotiate and on options is that on mode still sends out DTP frames, and the non-negotiate option does not. The non-negotiate option should be used for all VLAN trunks to minimize unnecessary network traffic for virtual switches in VST mode.

**Computing Check:** Request of copy of the external switch configuration that the ESX Server has trunk links configured. Work with the network reviewer and system administrator to verify the non-negotiate option is set.

For the Cisco CATOS the switch configuration should look similar to the following:

CATOS Console> (enable) set trunk <port number> nonnegotiate dot1q

For the Cisco IOS the switch configuration should look similar to the following:

IOS Console# switchport trunk nonnegotiate

If the non-negotiate option is not set, then this is a finding.

**Fix:** Configure the non-negotiate option for trunks connected to external physical switches.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0310:** Undocumented VLANs are configured on ESX Server in VST mode

**Vulnerability Key:** V0015822

**STIG ID:** ESX0310

**Vulnerability:** Undocumented VLANs are configured on ESX Server in VST mode.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** When defining a physical switch port for trunk mode, care must be taken to ensure only specified VLANs are configured. It is considered best practice to restrict only those VLANs required on the VLAN trunk link.

**Computing Check:**

1. Request from the IAO/SA the documentation that details the VLANs configured on the physical switch port to the ESX Server.
  2. Request a copy of the external switch port configurations to verify the documented VLANs match the configured VLANs.
- If there are undocumented VLANs configured on the external switch ports, then this is a finding.

**Fix:** Document all trunk VLANs between ESX Server and external switches.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0320:** ESX Server firewall is not configured to High Security

**Vulnerability Key:** V0015824

**STIG ID:** ESX0320

**Vulnerability:** ESX Server firewall is not configured to High Security.

**IA Controls:** DCP-1 Ports, Protocols, and Services, ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

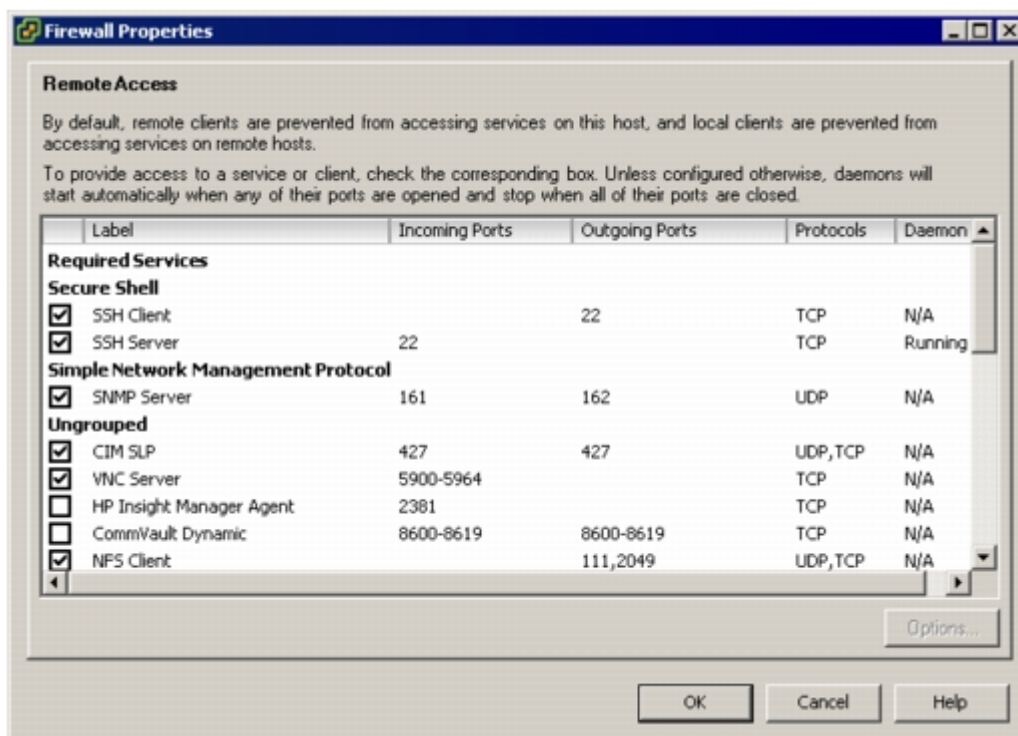
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** ESX Server includes a built in firewall between the service console and the network. To ensure the integrity of the service console, VMware has reduced the number of firewall ports that are open by default. At installation time, the service console firewall is configured to block all incoming and outgoing traffic except for ports 902, 80, 443, and 22, which are used for basic communication with ESX Server. This setting enforces a high level of security for the ESX Server host. Medium Security blocks all incoming traffic except on the default ports (902, 443, 80, and 22), and any ports users specifically open. Outgoing traffic is not blocked. Low Security does not block either incoming or outgoing traffic. This setting is equivalent to removing the firewall. Because the ports open by default on the ESX Server are strictly limited, additional ports may need to be open after installation for third party applications such as management, storage, NTP, etc. For instance, a backup agent may use specific ports such as 13720, 13724, 13782, and 13783.

**Computing Check:**

1. Log into VirtualCenter with the VI Client and select the ESX server from the inventory panel.
2. Click the Configuration tab and click Security Profile.  
The VI Client displays a list of currently active incoming and outgoing connections with the corresponding firewall ports.
3. Click Properties to open the Properties dialog box.  
The Firewall Properties dialog box lists all the services and management agents that are configured for the host. See figure below.



4. If you do not see the Firewall Properties window, then check proceed to step 7.
5. Review the services enabled to ensure that only the following ports are open:  
Ports that may be open for High Security: 902, 80, 443, and 22. If only these ports are open, then this is not a finding.
6. If there are other ports that are open, request the documentation from the IAO/SA that details the reasons for the additional ports are required. If no documentation can be produced, then this is a finding.
7. Verify IPtables are configured on the ESX Server service console by performing the following:

```
# iptables -L | grep hostd
```

The displayed result should look similar to the following:

```
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 443 -j Accept //hostd
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 80 -j Accept //hostd
```

```
# iptables -L | grep authd
```

The displayed result should look similar to the following:

```
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 902 -j Accept //authd
```

```
# iptables -L | grep snmpd
```

The displayed result should look similar to the following:

```
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 161 -j Accept //snmpd
```

At the bottom of the INPUT chain you should see the following:

```
iptables -A INPUT -j REJECT //deny all rule at end of chain
```

If no rules are applied to the INPUT chain for these services, then this is a finding.

If this cannot be verified, then this is a finding.

**Caveat:** Medium Security may be used only if additional ports are required to be open and it has been approved and documented by the IAO/SA.

**Fix:** Configure the ESX Server firewall to High Security.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0330:** A third party firewall is configured on ESX Server

**Vulnerability Key:** V0015825

**STIG ID:** ESX0330

**Vulnerability:** A third party firewall is configured on ESX Server.

**IA Controls:** DCPD-1 Use of Software, ECSC-1 Security Configuration Compliance

**Categories:** 12.8 Unsupported Vendor Products

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Third party software and services should not be installed in the service console. The service console is not intended to support the operation of additional software or services beyond what is included in the default ESX installation. VMware does not support the addition of third party applications that have not been explicitly approved.

**Non-Computing Check:** Ask the IAO/SA if any third party firewalls are installed on the ESX Server service console. If the answer is yes, inquire as to what is installed. If it is anything other than IPtables, then this is a finding.

**Fix:** Remove third party firewalls from the ESX Server service console.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0340:** IPtables or internal router/firewall is not configured to restrict IP addresses to services

**Vulnerability Key:** V0015826

**STIG ID:** ESX0340

**Vulnerability:** IPtables or internal router/firewall is not configured to restrict IP addresses to services.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The service console is a privileged virtual machine with interfaces into the VMkernel. In earlier releases, the service console was the main interface, whereas in ESX Server 3 and later, the VI Client is the primary interface. The service console is now used for advanced administration and system management functions such as HTTP, SNMP, and API interfaces. There are several processes and services that run in the service console which include the following: hostd, authd, net-snmp. To protect these important services on the service console, access control lists will be utilized to ensure only authorized IP addresses are able to access these services.

**Computing Check:**

1. If check ESX0320 was not a finding, then this check is not a finding. If it was a finding, then proceed to step 2.
2. Ask the IAO/SA what device is being used to restrict these services. If it is a router or firewall, then work with the network reviewer or system administrator to verify compliance.



3. If it is not a router/firewall, then review the IPtables configuration. Verify IPtables are configured on the ESX Server service console by performing the following:

```
# iptables -L | grep hostd
```

The displayed result should look similar to the following:

```
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 443 -j Accept //hostd
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 80 -j Accept //hostd
```

```
# iptables -L | grep authd
```

The displayed result should look similar to the following:

```
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 902 -j Accept //authd
```

```
# iptables -L | grep snmpd
```

The displayed result should look similar to the following:

```
iptables -A INPUT -d <IP Addresses Allowed> -p tcp -dport 161 -j Accept //snmpd
```

At the bottom of the INPUT chain you should see the following:

```
iptables -A INPUT -j REJECT //deny all rule at end of chain
```

If no rules are applied to the INPUT chain for these services, then this is a finding.

If this cannot be verified, then this is a finding.

**Note:** ESX Server 3.x uses hostd for the server daemon and it is not configurable with TCP wrappers. Hostd listens on http/https ports.

**Fix:** Restrict access to the ESX Server services to only authorized IP addresses.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0350:** ESX Server required services are not documented

**Vulnerability Key:** V0015827

**STIG ID:** ESX0350

**Vulnerability:** ESX Server required services are not documented.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Once the ESX Server is configured and operating, all required services needed for operation will be documented. Undocumented services running on the ESX Server opens up ports and vulnerabilities that may be exploited to gain access to the server. These services also consume processor cycles and memory. The ESX Server shares resources with virtual machines and the service console, and all excess resources are allocated based on the priorities configured.

**Computing Check:** Request the required services documentation from the IAO/SA. If no documentation can be produced, then this is a finding. Compare this to the services running on the ESX Server by performing the following on the service console:

#netstat -an

If a discrepancy exists between the services documented, and the services running, then this is a finding.

**Fix:** Document all required services for the ESX Server.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0360:** ESX Server service console users are not documented

**Vulnerability Key:** V0015828

**STIG ID:** ESX0360

**Vulnerability:** ESX Server service console users are not documented.

**IA Controls:** ECSC-1 Security Configuration Compliance, IAAC-1 Account Control

**Categories:** 1.3 Identity Management

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** User access to the service console should be restricted. The service console has privileged access to the ESX Server and only authorized users should be provided logon access. Personnel that manage the ESX Server will have individual usernames for accessing the ESX Server, creating an audit trail of activities. Virtual machine users will not have ESX Server logins, since there is no inherent need.

**Computing Check:** Request the ESX Server service console user documentation from the IAO/SA. Compare this documentation to the users on the ESX Server by performing the following at the service console:

```
#less /etc/passwd
```

If a discrepancy exists between the ESX Server and the documentation, then this is a finding.

**Fix:** Document all ESX Server service console users for the ESX Server.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0370:** Hash signatures for the /etc files are not stored offline

**Vulnerability Key:** V0015829

**STIG ID:** ESX0370

**Vulnerability:** Hash signatures for the /etc files are not stored offline.

**IA Controls:** ECCT-1 Encryption for Confidentiality, ECCT-2 Encryption for Confidentiality

**Categories:** 8.5 Hashing

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Several files within ESX Server should be checked for file system integrity periodically. These files have been deemed critical by VMware in maintaining file system integrity. System administrators must ensure these files have the correct permissions and have not been modified. To ensure integrity, system administrators will use a FIPS 140-2 hash algorithm to create signatures of these files and store them offline. Comparing these hash values periodically will verify the integrity of the files.

**Computing Check:** The following /etc files in the table below need to have hash signatures that are stored offline. Ask the IAO/SA the location of the hash signatures and verify that it is not on the ESX Server host. If it is, then this is a finding. If the hash signatures are incomplete, then this is a finding.

File Location	Permission
/etc/fstab	640
/etc/group	644
/etc/host.conf	640
/etc/hosts	640
/etc/hosts.allow	640
/etc/hosts.deny	640
/etc/logrotate.conf	640
/etc/logrotate.d/	700
/etc/modules.conf	640
/etc/motd	640
/etc/ntp	755
/etc/ntp.conf	644
/etc/pam.d/system-auth	644
/etc/profile	644
/etc/shadow	400
/etc/securetty	600
/etc/ssh/sshd_config	600
/etc/snmp	755
/etc/sudoers	440
/etc/vmware	755

**Fix:** Store the hash signatures for the /etc files in an offline location.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0380:** Hash signatures for the /etc files are not reviewed monthly

**Vulnerability Key:** V0015833

**STIG ID:** ESX0380

**Vulnerability:** Hash signatures for the /etc files are not reviewed monthly.

**IA Controls:** ECCT-1 Encryption for Confidentiality, ECCT-2 Encryption for Confidentiality

**Categories:** 8.5 Hashing

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Several files within ESX Server should be checked for file system integrity periodically. These files have been deemed critical by VMware in maintaining file system integrity. System administrators must ensure these files have the correct permissions and have not been modified. To ensure integrity, system administrators will use a FIPS 140-2 hash algorithm to create signatures of these files and store them offline. Comparing these hash values periodically will verify the integrity of the files.

**Non-Computing Check:** Ask the IAO/SA how often the hash signatures are reviewed. If they are not reviewed at least monthly, then this is a finding.

File Location	Permission
/etc/fstab	640
/etc/group	644
/etc/host.conf	640
/etc/hosts	640
/etc/hosts.allow	640
/etc/hosts.deny	640

/etc/logrotate.conf	640
/etc/logrotate.d/	700
/etc/modules.conf	640
/etc/motd	640
/etc/ntp	755
/etc/ntp.conf	644
/etc/pam.d/system-auth	644
/etc/profile	644
/etc/shadow	400
/etc/securetty	600
/etc/ssh/sshd_config	600
/etc/snmp	755
/etc/sudoers	440
/etc/vmware	755

**Fix:** Review the hash signatures for the /etc files monthly.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0390:** The setuid and setgid flags have been disabled

**Vulnerability Key:** V0015835

**STIG ID:** ESX0390

**Vulnerability:** The setuid and setgid flags have been disabled.

**IA Controls:** IAIA-1, IAIA-2, IAAC-1

**Categories:** 1.3 Identity Management

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** During the ESX Server installation, several applications have the setuid and setgid flags set by default. These applications are initiated by or through the service console. Some of them provide facilities required for correct operation of the ESX Server host. Others are optional, but can make maintaining and troubleshooting the ESX Server and network easier. Disabling any of the required setgid or setuid applications will result in problems with ESX Server authentication and virtual machine operation; however optional setgid or setuid applications may be disabled.

**Computing Check:** All the following setuid applications should have the suid bit configured so that normal users may run the application with raised privileges. The output of the following commands should look similar to the following:

**-r-Sr-Xr-X**

To verify the suid bit is set (s), perform the following on the ESX Server service console:

```
#cd /sbin/  
#ls -l | grep pam_timestamp_check  
#ls -l | grep pwdb_chkpwd  
#ls -l | grep unix_chkpwd
```

```
#cd /usr/bin/  
#ls -l | grep crontab  
#ls -l | grep passwd
```

```
#cd /bin/  
#ls -l | grep su
```

```
#cd /usr/lib/vmware/bin/  
#ls -l | grep vmkload_app  
#ls -l | grep vmware-vmx
```

```
#cd /usr/lib/vmware/bin-debug/  
#ls -l | grep vmkload_app  
#ls -l | grep vmware-vmx
```

```
#cd /usr/sbin/  
#ls -l | grep vmware-authd
```

If the setuid bit is not set on these applications, then this is a finding.

**Fix:** Do not disable the setuid and setgid applications.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0400:** ESX Server is not authenticating the time source with a hashing algorithm

**Vulnerability Key:** V0015836

**STIG ID:** ESX0400

**Vulnerability:** ESX Server is not authenticating the time source with a hashing algorithm.

**IA Controls:** ECCT-1 Encryption for Confidentiality, ECCT-2 Encryption for Confidentiality

**Categories:** 8.5 Hashing

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Since NTP is used to ensure accurate log file timestamps for information, NTP could pose a security risk if a malicious user were able to falsify NTP information. Implementing authentication between NTP peers can mitigate this risk. When hashing authentication is enforced, there is a greater level of assurance that NTP updates are from a trusted source.

**Computing Check:** NTP authentication is used by time clients to authenticate the time server to prevent rogue server intervention. NTP authentication is based on encrypted keys. A key is encrypted and sent to the client by the server, where it is unencrypted and checked against the client key to ensure a match.

NTP keys are stored in the 'ntp.keys' file in the following format:

Key-number M Key (The M stands for MD5 encryption), e.g.:

1 M secret

5 M RaBBit

7 M TiMeLy

10 M MYKEY

The NTP configuration file 'ntp.conf' specifies which of the keys are trusted. Any keys specified in the keys file but not trusted will not be used for authentication, e.g.:

trustedkey 1 7 10

In this example, 5 is not trusted, only 1, 7, and 10 above.

1. On the ESX Server service console perform the following:



```
#cd /etc
#cat ntp.conf
```

Review the configuration file to verify that the following are uncommented:

```
authenticate yes
....
keys /etc/ntp/keys
```

If these are commented out, then this is a finding.

2. Next verify that the trusted keys are configured in the ntp.conf file.

```
trustedkey <number>
```

If none are listed, then this is a finding.

3. Next, review the keys file located at /etc/ntp/keys by performing the following:

```
#cd /etc/ntp
#cat keys
```

Verify that keys are listed in the keys file. File should look similar to the following:

```
5 M RaBBit 7 M TiMeLy 10 M MYKEY
```

If no keys are configured here, then this is a finding.

**Fix:** Configure the ESX Server to authenticate the time source.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0410:** ESX Server does not record log files

**Vulnerability Key:** V0015840

**STIG ID:** ESX0410

**Vulnerability:** ESX Server does not record log files.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record

**Categories:** 10.4 Reporting

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Logs form a recorded history or audit trail of the ESX Server system events, making it easier for system administrators to track down intermittent problems, review past events, and piece together information if an investigation is required. Without this recorded history, potential attacks and suspicious activity will go unnoticed.

ESX Server log files that are critical to record include VMkernel, VMkernel warnings, VMkernel summary, ESX Server host agent, virtual machines, VI Client agent, Web Access, service console, and authentication. The VMkernel logs record activities related to the virtual machines and the ESX Server. The VMkernel warning log file records activities with the virtual machines. The VMkernel summary is used to determine uptime and availability statistics for the ESX Server. The ESX Server host agent log contains information on the agent that manages and configures the ESX Server host. This log may assist in diagnosing connection problems. The virtual machine log files contain information when a virtual machine crashes or shutdowns abnormally. The VI Client agent is installed on each managed ESX Server and this log records all the activities of the agent. Web Access records information on web-based access to the ESX Server. This is important to view since web-based access to the ESX Server should be disabled. The service console messages contain all general log messages used to troubleshoot virtual machines or the ESX Server. The authentication log contains records of connections that require authentication.

**Computing Check:**

To verify that all the log files are being written to, perform the following on the ESX Server service console:

```
#cd /var/log
#less vmkernel
#less vmkwarning
#less vmksummary.txt
#less messages
#less secure
```

```
#cd /var/log/vmware/
#less vpxa.log
#less webAccess
```

Work with SA to locate the path to the virtual machines.

```
#cd <path to virtual machine on ESX Server>/
#less vmware.log
```

**Caveat:** If logs are being sent to a syslog server, then work with the system administrator to verify they are being written to.

Location of all logs to be verified are listed below:

VMkernel

/var/log/vmkernel

VMkernel warnings:

/var/log/vmkwarning

VMkernel summary:

/var/log/vmksummary.txt

ESX Server host agent log:

/var/log/vmware/hostd.log

Individual virtual machine logs:

<path to virtual machine on ESX Server>/vmware.log

VI Client agent log:

/var/log/vmware/vpx/vpxa.log

Web access:

/var/log/vmware/webAccess

Service console:

/var/log/messages

Authentication log:

/var/log/secure

**Fix:** Record all critical log files on the ESX Server.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0420:** ESX Server log files are not reviewed daily

**Vulnerability Key:** V0015841

**STIG ID:** ESX0420

**Vulnerability:** ESX Server log files are not reviewed daily.

**IA Controls:** ECAT-1 Audit, Trail, Monitoring, Analysis, and Reporting, ECAT-2 Audit, Trail, Monitoring, Analysis, and Reporting

**Categories:** 10.3 Review

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

## Severity: Category II

**Vulnerability Discussion:** Logs form a recorded history or audit trail of the ESX Server system events, making it easier for system administrators to track down intermittent problems, review past events, and piece together information if an investigation is required. Without this recorded history, potential attacks and suspicious activity will go unnoticed.

ESX Server log files that are critical to record include VMkernel, VMkernel warnings, VMkernel summary, ESX Server host agent, virtual machines, VI Client agent, Web Access, service console, and authentication. The VMkernel logs record activities related to the virtual machines and the ESX Server. The VMkernel warning log file records activities with the virtual machines. The VMkernel summary is used to determine uptime and availability statistics for the ESX Server. The ESX Server host agent log contains information on the agent that manages and configures the ESX Server host. This log may assist in diagnosing connection problems. The virtual machine log files contain information when a virtual machine crashes or shutdowns abnormally. The VI Client agent is installed on each managed ESX Server and this log records all the activities of the agent. Web Access records information on web-based access to the ESX Server. This is important to view since web-based access to the ESX Server should be disabled. The service console messages contain all general log messages used to troubleshoot virtual machines or the ESX Server. The authentication log contains records of connections that require authentication.

**Non-Computing Check:** Ask the IAO/SA how often they review the ESX Server log files listed below:

VMkernel

/var/log/vmkernel

VMkernel warnings:

/var/log/vmkwarning

VMkernel summary:

/var/log/vmksummary.txt

ESX Server host agent log:

/var/log/vmware/hostd.log

Individual virtual machine logs:

<path to virtual machine on ESX Server>/vmware.log

VI Client agent log:

/var/log/vmware/vpx/vpxa.log

Web access:

/var/log/vmware/webAccess

Service console:

/var/log/messages

Authentication log:

/var/log/secure

**Caveat:** If the log files are being written to a syslog server, then work with the system administrator to verify they are being reviewed there.

If the IAO/SA does not review them daily, then this is a finding.

**Fix:** Review ESX Server log files daily.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0430:** Log file permissions have not been configured to restrict unauthorized users

**Vulnerability Key:** V0015842

**STIG ID:** ESX0430

**Vulnerability:** Log file permissions have not been configured to restrict unauthorized users.

**IA Controls:** ECCD-1, ECCD-2 Changes to Data, ECAN-1 Access to Need to Know

**Categories:** 2.1 Object Permissions

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** It is critical to protect system log files from being modified or accessed by unauthorized individuals. Some logs may contain sensitive data that should only be available to the virtualization server administrator.

**Computing Check:**

On the ESX Server service console verify that the following log file permissions have not been modified.

For each file or folder perform the following:

#cd /var/log/

#ls -lL <file or directory>

Log Location	Permission
/var/log/boot.log	600

/var/log/cron	600
/var/log/dmesg	640
/var/log/initrdlogs/	600
/var/log/ksyms	600
/var/log/maillog	600
/var/log/messages	600
/var/log/oldconf/	700
/var/log/rpmpkgs	600
/var/log/secure	600
/var/log/spooler	600
/var/log/storageMonitor	600
/var/log/sudolog	600
/var/log/vmkernel	600
/var/log/vmkproxy	600
/var/log/vmksummary	600
/var/log/vmksummary.d/	600
/var/log/vmkwarning	600
/var/log/vmware/	700

If any of the directories or files do not match the table above, then this is a finding.

**Fix:** Restrict unauthorized users from log files.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0440:** ESX Server does not send logs to a syslog server

**Vulnerability Key:** V0015843

**STIG ID:** ESX0440

**Vulnerability:** ESX Server does not send logs to a syslog server.

**IA Controls:** ECRR-1 Audit Record Retention

**Categories:** 10.4 Reporting, 10.5 Retention

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Remote logging is essential in monitoring servers and detecting intrusion. If an intruder is able to obtain root on a host, they may be able to edit the system logs to remove all traces of the attack. If the logs are stored off the machine, those logs can be analyzed for suspicious activity and used for prosecuting the attacker. Centralized log monitoring and storage is a critical component of incident response and assuring the integrity of system logs.

Redundancy is important when considering using a virtual machine for a syslog server. If the syslog virtual machine is hosted on only one ESX Server, and the ESX Server fails, all logging to the syslog server will cease. Configuring the syslog server as a virtual machine requires proper failover planning in case the primary ESX Server would fail. To mitigate this scenario, syslog virtual machines will be configured within ESX Server farms with High Availability (HA) enabled.

**Computing Check:**

1. To determine if the ESX Server is sending its logs to a remote syslog server, examine the /etc/syslog.conf file on the ESX Server service console.
2. To send all syslog data from the ESX Server to a remote syslog host, search for the following line(s) in the /etc/syslog.conf file:

\*.\* <Tab><Tab> @loghost (name of remote host)

Or

\*.debug, info, etc.@loghost.

At a minimum, the following log files should be configured to send logs to the syslog server:

<u>Log Name</u>	<u>Facility.Level</u>	<u>Default Location</u>
Service Console Logs	*.info	/var/log/messages
Authentication Logs	Authpriv.*	/var/log/secure
VMkernel Logs	Local6.notice	/var/log/vmkernel
VMkernel Warnings	Local6.warning	/var/log/vmkwarning

If these are not configured to the syslog server, then this is a finding.

3. Verify the loghost referred to in the syslog.conf file is not resolving to the localhost. Check /etc/hosts file to review what the remote host is referring to. If it is not in this file, then check the DNS server to determine what it is resolving to. If it is resolving to localhost, then this is a finding.

**Caveat:** This syslog server may be a virtual machine within an ESX Server farm with HA enabled. If the syslog server is a virtual machine within a server farm and HA is not enabled, then this is a finding. It may not be a virtual machine if there is only one ESX Server for the site. If this is the case, then this is a finding.

**Fix:** Configure the ESX Server to send all its logs to a syslog server.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0450:** Auditing is not configured on the ESX Server

**Vulnerability Key:** V0015844

**STIG ID:** ESX0450

**Vulnerability:** Auditing is not configured on the ESX Server.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record Retention

**Categories:** 10.4 Reporting

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Audit utilities can extract information about specific users and processes from the audit files. The IAO/SA will ensure audit files are only accessible to authorized personnel. Auditing will be configured to immediately alert personnel of any unusual or inappropriate activity with potential IA implications. All users, including root, will be audited. The system administrator will rotate and compress the audit logs one or more times a day to reduce space and the time required for log searches and reviews. Audit data will be backed up weekly onto a different system or media than the system being audited. Utilizing an audit server will ease the attention required by audit logs and provide compliance with the requirement for the backup of audit data.

Auditing will be configured according to section 3.16 of the UNIX STIG. Audit logs and audit files must be analyzed at regular intervals. Such files can quickly grow to large proportions. To keep the size of log files and audit files within a useful range, the evaluation intervals should not be impractically short, but short enough to allow a clear examination. Collected data will be



examined and analyzed daily to detect any compromise or attempted compromise of system security.

**Computing Check:**

On the ESX Server service console perform the following command:

```
#ps -ef | grep auditd
```

Verify the auditd daemon is running. If it is not, then this is a finding.

**Fix:** Configure LAUS on the ESX Server.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0460:** The IAO/SA does not subscribe to vendor security patches and update notifications

**Vulnerability Key:** V0015845

**STIG ID:** ESX0460

**Vulnerability:** The IAO/SA does not subscribe to vendor security patches and update notifications.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 3.1 Security Patches, 3.2 Operational / PM Patches

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Organizations need to stay current with all applicable ESX Server software updates that are released from VMware. In order to be aware of updates as they are released, virtualization server administrators will subscribe to ESX Server vendor security notices, updates, and patches to ensure that all new vulnerabilities are known. New ESX Server patches and updates should be reviewed for the ESX Server before moving them into a production environment.

**Non-Computing Check:** Ask the IAO/SA to provide actual update notification to verify that they are on the subscription list. The email subscription for VMware is security-

announce@lists.vmware.com. If no emails or documentation can be provided, then this is a finding.

**Fix:** Subscribe to vendor security and patch notifications.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0470:** The ESX Server software version is not at the latest release

**Vulnerability Key:** V0015846

**STIG ID:** ESX0470

**Vulnerability:** The ESX Server software version is not at the latest release.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 3.1 Security Patches, 3.2 Operational / PM Patches

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Organizations need to stay current with all applicable ESX Server software updates that are released from VMware. Software updates are designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics and improving the usability or performance. ESX Servers that do not have the latest patches or updates installed have potential vulnerabilities that may be exploited.

### Computing Check:

On the ESX Server service console perform the following:

# esxupdate -l query

The output will look similar to the following:

```
Installed software bundles
-----Name-----  --Install Date--  -----Summary-----
3.5.0-56329          23:37:26 11/04/08    Full installation of ESX 3.5.0-56329
ESX350-200802055-BG  23:49:26 11/04/08    Fix COS running Dell OM5 w/QLogic
ESX350-200803066-SG  23:50:02 11/04/08    Fix COS security bug
```

Verify the latest release is listed. The latest release for the various software versions is listed:

Version 3.5.0 - ESX350-200712401-BG

Version 3.0.2 Update 1 - ESX-1003359

Version 3.0.2 - ESX-1003359 (End of support is 10/29/2008)

Version 3.0.1 - ESX-1003347 (End of support is 7/31/2008)

Version 3.0.0 – Not Supported by VMware

Version 2.5.5 – Update Patch 4 (End of support 6/15/2010)

Version 2.5.4 – Update Patch 15 (End of Support is 10/8/2008)

Patches are released monthly, so check VMware's website to ensure new patches have not been released. The website for patch downloads is <http://www.vmware.com/download/vi/>.

If the latest release is not installed, then this is a finding.

**Fix:** Configure the ESX Server software with the latest release.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0480:** ESX Server updates are not tested

**Vulnerability Key:** V0015847

**STIG ID:** ESX0480

**Vulnerability:** ESX Server updates are not tested.

**IA Controls:** DCCT-1 Deployment Procedures

**Categories:** 3.1 Security Patches, 3.2 Operational / PM Patches

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Organizations need to stay current with all applicable ESX Server software updates that are released from VMware. In order to be aware of updates as they are released, virtualization server administrators will subscribe to ESX Server vendor security notices, updates, and patches to ensure that all new vulnerabilities are known. New ESX Server

patches and updates should be reviewed for the ESX Server before moving them into a production environment. ESX Server patches will be tested first in a development environment and any issues or special precautions will be documented, as a patch could technically disable all virtual networks and machines.

**Computing Check:** Ask the IAO/SA to show you where the test and development ESX Server is located. At the service console of the test and development ESX Server perform the following command:

#esxupdate -l query

The output will look similar to the following:

```
Installed software bundles
-----Name-----  --Install Date--  -----Summary-----
3.5.0-56329          23:37:26 11/04/08  Full installation of ESX 3.5.0-56329

ESX350-200802055-BG  23:49:26 11/04/08  Fix COS running Dell OM5 w/QLogic

ESX350-200803066-SG  23:50:02 11/04/08  Fix COS security bug
```

If no patch results are returned, then this is a finding.

The test and development ESX Server cannot be the production ESX Server(s).

**Fix:** Use the test and development ESX Server to test all patches before moving them to production.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0490:** VMware tools are not used to update the ESX Server

**Vulnerability Key:** V0015848

**STIG ID:** ESX0490

**Vulnerability:** VMware tools are not used to update the ESX Server.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** VMware uses three categories for patches: Security, Critical, and General. VMware will usually issue a KB article when they become aware of security vulnerabilities and other serious functionality issues before they issue a patch. Only VMware released patches and tools (such as `esxupdate`) should be implemented. Do not use RedHat or third party patches or tools such as `yum` or `rpm` to update the system because VMware has made modifications to the system and kernel.

**Computing Check:** On the ESX Server service console perform the following commands:

```
#cd /var/log/vmware
```

```
#less esxupdate.log | grep esxupdate
```

If no entries are returned, then this is a finding.

**Fix:** Utilize VMware tools for all ESX Server updates.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0500:** ESX Server software version is not supported

**Vulnerability Key:** V0015849

**STIG ID:** ESX0500

**Vulnerability:** ESX Server software version is not supported.

**IA Controls:** ECSC-1 Security Configuration Guide

**Categories:** 12.8 Unsupported Vendor Products

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category I

**Vulnerability Discussion:** ESX Servers require support for release versions, management applications, and the guest operating systems in the virtual machine. The ESX Server runs on its own hypervisor/kernel which is supported by the VMware's technical support. The ESX Server

will be a supported release to ensure the release may be patched. This will ensure the ability to comply with IAVM requirements as well as access to vendor recommended and security patches.

### Computing Check:

On the ESX Server service console perform the following:

```
# esxupdate -l query
```

Output will look similar to this:

```
Installed software bundles
-----Name-----  --Install Date--  -----Summary-----
3.5.0-56329          23:37:26 11/04/08  Full installation of ESX 3.5.0-56329  - This is
the line to assess what ESX software version is installed.

ESX350-200802055-BG  23:49:26 11/04/08  Fix COS running Dell OM5 w/QLogic
ESX350-200803066-SG  23:50:02 11/04/08  Fix COS security bug
```

Check VMware's website to double check the support policy in case it has been updated if you have access to the internet. The URL is

[http://www.vmware.com/support/policies/eos\\_vi.html#General](http://www.vmware.com/support/policies/eos_vi.html#General)

Below is the support schedule for the various release of the ESX Server. If the esxupdate -l query return anything below 2.5.4, then this is a finding. If the query returns 3.0.0, then this is a finding. For all other results, check the schedule and date for end of support to determine if this check is a finding.

VMware ESX Server	General Availability Date	End of Support (Security and Bug fixes)	Note
Version 3.0.2 Update 1	10/29/2007	One year after Version 3.0.2 Update 2 GA	
Version 3.0.2	07/31/2007	10/29/2008	
Version 3.0.1	10/05/2006	07/31/2008	
Version 3.0.0	06/15/2006	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<hr/>			
Version 2.5.5	10/08/2007	06/15/2010, pending no Version 2.5.6 release	
Version 2.5.4	10/05/2006	10/08/2008	
Version 2.5.3	04/13/2006	EOS Reached	Not covered by VI Support Life Cycle, see FAQ

<b>Version 2.5.2</b>	09/15/2005	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<b>Version 2.5.1</b>	06/20/2005	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<b>Version 2.5.0</b>	11/29/2004	EOS Reached	Not covered by VI Support Life Cycle, see FAQ

**Fix:** Implement only VMware supported ESX Server software.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0510:** VMware and third party applications are not supported

**Vulnerability Key:** V0015850

**STIG ID:** ESX0510

**Vulnerability:** VMware and third party applications are not supported.

**IA Controls:** ECSC-1 Security Configuration Guide

**Categories:** 12.8 Unsupported Vendor Products

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category I

**Vulnerability Discussion:** ESX Servers require support for release version, management applications, and the guest operating systems in the virtual machine. The ESX Server runs on its own hypervisor/kernel which is supported by the VMware's technical support. VMware and third party applications will be a supported release to ensure the release may be patched. This will ensure the ability to comply with IAVM requirements as well as access to vendor recommended and security patches.

**Computing Check:** There are many third party applications that may be used in conjunction with VI3. There are many VMware applications that may be used to enhance the virtualization infrastructure. These include VMware Consolidated Backup, VirtualCenter, VMotion, Hardware Availability, and Distributed Resource Scheduling.

1. Request the list of all the VMware and third party applications used in the virtualization infrastructure. Use this list to research the support of each product. If no list can be produced then this is a finding.
2. For all third party applications, go to the vendor's website or request from the IAO/SA documentation verifying that the application is supported. If the application is not supported, then this is a finding.
3. For VMware applications, look at the table and end of support dates below. Check VMware's website to double check the support policy in case it has been updated if you have access to the internet. The URL is [http://www.vmware.com/support/policies/eos\\_vi.html#General](http://www.vmware.com/support/policies/eos_vi.html#General)  
If the VMware application is not supported, then this is a finding.

VMware Consolidated Backup	General Availability Date	End of Support (Security and Bug fixes)	Note
Version 1.0.3 Update 1	10/31/2007	One year after Version 1.0.3 Update 2 GA	
Version 1.0.3	07/31/2007	10/31/2008	
Version 1.0.2 Update 1	10/31/2007	07/31/2008	
Version 1.0.2	04/05/2007	10/31/2008	
Version 1.0.1	10/02/2006	04/05/2008	
Version 1.0.0	06/15/2006	EOS Reached	Not covered by VI Support Life Cycle, see FAQ

VMware VirtualCenter, VMware Vmotion, VMware HA, and VMware DRS	General Availability Date	End of Support (Security and Bug fixes)	Note
Version 2.0.2 Update 2	11/08/2007	One year after Version 2.0.2 Update 3	
Version 2.0.2 Update 1	10/29/2007	11/08/2008	
Version 2.0.2	07/19/2007	10/29/2008	
Version 2.0.1	10/05/2006	07/19/2008	



<b>Version 2.0.0</b>	06/15/2006	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<hr/>			
<b>Version 1.4.1</b>	09/28/2006	06/15/2010, pending no Version 1.4.2	
<b>Version 1.4.0</b>	07/06/2006	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<hr/>			
<b>Version 1.3.1 P1</b>	03/23/2006	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<b>Version 1.3.1</b>	12/22/2005	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<b>Version 1.3.0</b>	09/22/2005	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<hr/>			
<b>Version 1.2.0 P1</b>	02/24/2005	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<b>Version 1.2.0</b>	12/19/2004	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<hr/>			
<b>Version 1.1.0</b>	08/06/2004	EOS Reached	Not covered by VI Support Life Cycle, see FAQ
<hr/>			
<b>Version 1.0.0</b>	03/31/2004	EOS Reached	Not covered by VI Support Life Cycle, see FAQ

**Fix:** Use only vendor supported products with the virtualization infrastructure.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0520:** There are no backup and recovery procedures

**Vulnerability Key:** V0015851

**STIG ID:** ESX0520

**Vulnerability:** There are no procedures for the backup and recovery of the ESX Server, management servers, and virtual machines.

**IA Controls:** DCSD-1 IA Documentation

**Categories:** 13.4 Backup & Recovery

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Backup and recovery procedures are critical to the availability and protection of the virtual infrastructure. Availability of the system will be hindered if the system is compromised, shutdown, or not available. Backup and recovery of the virtual environment includes the ESX Servers, management servers, and virtual machines. The ESX Server has three major components required for backup and recovery. These components are virtual disks, virtual machine configuration files, and the configuration of the ESX Server itself. Due to the array of products and options available to backup the virtualization infrastructure, procedures will need to be developed to provide guidance to system administrators.

**Non-Computing Check:** Request a copy of the backup and recovery procedures for the ESX Servers, management applications, and virtual machines. If no procedures can be produced or they are incomplete, then this is a finding.

**Fix:** Develop backup and recovery procedures for the virtual infrastructure.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0530:** The ESX Servers and management servers are not backed up

**Vulnerability Key:** V0015852

**STIG ID:** ESX0530

**Vulnerability:** The ESX Servers and management servers are not backed up in accordance to the MAC level of the servers.

**IA Controls:** CODB-1, CODB-2, CODB-3 Data Backup

**Categories:** 13.4 Backup and Recovery

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Backups of the ESX Server and management servers are critical in order to recover from hardware problems, unexpected software errors, or a disaster to the computing facility. Data backup must be performed in accordance with its mission assurance category (MAC) level. For MAC III systems it is necessary to ensure that backups are performed weekly. For MAC II systems backups are performed daily and the recovery media is stored off-site in a protected facility in accordance with its mission assurance category and confidentiality level. In MAC I systems backups are maintained through a redundant secondary system which is not collocated, and can be activated without loss of data or disruption to the operation.

**Computing Check:**

1. Determine the MAC level of the ESX and management servers by asking the IAO/SA.
2. Once the MAC level is determined, locate the backup media or storage location.  
For MAC I servers, a redundant secondary system is required that is not collocated.  
For MAC II servers, daily backups are required with recovery media stored offline.  
For MAC III servers, backups must be performed weekly.
3. Depending on the MAC level, verify the servers are backed up to media or storage within the guidelines of the MAC level. If they are not, then this is a finding.

**Fix:** Backup the ESX and management servers in accordance to the MAC level.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0540:** Disaster recovery plan does not include virtual infrastructure

**Vulnerability Key:** V0015853

**STIG ID:** ESX0540

**Vulnerability:** Disaster recovery plan does not include ESX Servers, VirtualCenter servers, virtual machines, and necessary peripherals associated with the system.

**IA Controls:** CODP-1, CODP-2, CODP-3 Disaster Recovery Plan

**Categories:** 13.4 Backup and Recovery

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Disaster and recovery plans should be drafted and exercised in accordance with the MAC level of the system/Enclave as defined by the DoDI 85002. Disaster plans provide for the resumption of mission or business essential functions. A disaster plan must exist that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance).

**Non-Computing Check:** Request a copy of the disaster recovery plan from the IAO/SA. Review the plan to verify that the ESX Server, management applications, virtual machines, and all necessary system peripherals are included in the plan. If the plan does not include the virtual infrastructure or is incomplete, then this is a finding.

**Fix:** Add the virtual infrastructure to the disaster recovery plan.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0550:** Backups are not located on separate logical partition from production data

**Vulnerability Key:** V0015854

**STIG ID:** ESX0550

**Vulnerability:** Backups are not located on separate logical partition from production data.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Since backups are critical to the recovery of the virtualization infrastructure, storing these files on the same logical location as the production servers is not recommended. The backup files will be stored on a separate logical partition so restoration is possible in case of any hardware failures on the production physical servers.

**Computing Check:** Ask the IAO/SA to show you the location of the backup data for the ESX Servers, VirtualCenter servers, virtual machines, and any other virtual infrastructure applications. If the backup data is on separate physical media, then this would not be a finding. If the backups are located on a SAN, verify that the production data is logically partitioned from the backup media. If the backup data is on the same partition as the production data, then this is a finding.

**Fix:** Place backup data on a separate partition from the production data.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0560:** VI client sessions to the ESX Server are unencrypted

**Vulnerability Key:** V0015855

**STIG ID:** ESX0560

**Vulnerability:** VI client sessions to the ESX Server are unencrypted.

**IA Controls:** ECCT-1, ECCT-2 Encryption of Transmitted Data

**Categories:** 8.1 Encrypted Data in Transit

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** User sessions with the ESX Server should be encrypted since transmitting data in plaintext may be viewed as it travels through the network. User sessions may be initiated from the VI client, Web Access, or through VirtualCenter. To encrypt session data, the sending component, such as a gateway or redirector, applies ciphers to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. To ensure the protection of the data transmitted to and from external network connections, ESX Server uses the 256-bit AES block encryption. ESX Server also uses 1024-bit RSA for key exchange. These encryption algorithms are the default for VI Client, VI Web Access, VirtualCenter sessions.

**Computing Check:**

1. Log into the VirtualCenter server using the VI Client.
2. Click Administration > VirtualCenter Management Server Configuration  
The VirtualCenter Management Server Configuration dialog appears.
3. Click SSL Settings in the left pane and enable Check host certificates checkbox. Click OK.  
If the Check host certificates checkbox is not checked, then this is a finding.
4. Verify that the SSL certificates exist on the ESX Server. On the ESX Server service console check the /etc/vmware/ssl/ directory for the certificates by performing the following:

```
#cd /etc/vmware/ssl/
```

```
#ls -lL
```

The output should look similar to the following:

```
rui.cert
```

```
rui.key
```

If this directory does not contain a cert and key file, then this is a finding.

**Fix:** Enable encryption for all VI client sessions with the ESX Server.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0570:** VI Web Access sessions to the ESX Server are unencrypted

**Vulnerability Key:** V0015856

**STIG ID:** ESX0570

**Vulnerability:** VI Web Access sessions to the ESX Server are unencrypted.

**IA Controls:** ECCT-1, ECCT-2 Encryption of Transmitted Data

**Categories:** 8.1 Encrypted Data in Transit

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** User sessions with the ESX Server should be encrypted since transmitting data in plaintext may be viewed as it travels through the network. User sessions may be initiated from the VI client, Web Access, or through VirtualCenter. To encrypt session data, the sending component, such as a gateway or redirector, applies ciphers to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. To ensure the protection of the data transmitted to and from external network connections, ESX Server uses the 256-bit AES block encryption. ESX Server also uses 1024-bit RSA for key exchange. These encryption algorithms are the default for VI Client, VI Web Access, and VirtualCenter sessions.

**Computing Check:**

1. First verify Web Access is enabled by having the IAO/SA attempt to login to the ESX Server.
2. Start the Web Browser
3. Enter the URL of the ESX Server: <http://<host or server name>/ui>. The http should transition to <https://<host or server name>/ui>. If it does not transition to https, then this is a finding.

**Fix:** Encrypt all Web Access session to ESX Servers.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0580:** VirtualCenter communications to the ESX Server are unencrypted

**Vulnerability Key:** V0015857

**STIG ID:** ESX0580

**Vulnerability:** VirtualCenter communications to the ESX Server are unencrypted.

**IA Controls:** ECCT-1, ECCT-2 Encryption of Transmitted Data

**Categories:** 8.1 Encrypted Data in Transit

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** User sessions with the ESX Server should be encrypted since transmitting data in plaintext may be viewed as it travels through the network. User sessions may be initiated from the VI client, Web Access, or through VirtualCenter. To encrypt session data, the sending component, such as a gateway or redirector, applies ciphers to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. To ensure the protection of the data transmitted to and from external network connections, ESX Server uses the 256-bit AES block encryption. ESX Server also uses 1024-bit RSA for key exchange. These encryption algorithms are the default for VI Client, VI Web Access, VirtualCenter sessions.

**Computing Check:**

On the ESX Server service console perform the following:

```
#cd /etc/vmware/hostd/  
# less config.xml | grep ssl  
<ssl>  
<privatekey>/etc/vmware/ssl/rui.key</privatekey>  
<certificate>/etc/vmware/ssl/rui.crt</certificate>  
</ssl>
```

If you do not see the private key and certificate listed between the SSL tags or the lines are commented out, then this is a finding.

**Fix:** Encrypt all VirtualCenter sessions with ESX Servers.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0590:** SNMP write mode is enabled on ESX Server

**Vulnerability Key:** V0015858

**STIG ID:** ESX0590

**Vulnerability:** SNMP write mode is enabled on ESX Server.

**IA Controls:** ECSC-1 Security Configuration Compliance



**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The Simple Network Management Protocol (SNMP) is an application-layer protocol used for exchanging management information between network devices. There are four types of SNMP commands that may be used to control and monitor managed devices. These include read, write, trap, and traversal operations. The read command is used to monitor devices, while the write command is used to configure devices and change device settings. The trap command is used to "trap" events from the device and report them back to the monitoring system. Traversal operations are used to determine the variables specific devices support.

The ESX Server SNMP package is setup by default in a secure configuration. The configuration has a single community string with read-only access which is the default mode. This is denoted by the "ro" community configuration parameter in the configuration file for the master snmpd daemon, snmpd.conf. Furthermore, the UNIX SRR scripts check for proper snmpd.conf and MIB permissions, and snmpd.conf and MIB ownership. They also check to ensure that the default community strings have been changed, and if there is a dedicated SNMP server configured.

**Computing Check:**

Log into the ESX Server service console and perform the following.

```
#cd /etc/snmp/
```

```
#less snmpd.conf | grep rwcommunity
```

If the command returns a result, then this is a finding.

**Fix:** Disable SNMP write mode.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0600:** VirtualCenter server is hosting other applications.

**Vulnerability Key:** V0015859

**STIG ID:** ESX0600

**Vulnerability:** VirtualCenter server is hosting other applications such as database servers, e-mail servers or clients, dhcp servers, web servers, etc.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** VirtualCenter availability is critical since it controls and manages the entire virtual infrastructure. ESX Server will still function without VirtualCenter, however, management of the virtual machines is lost. VirtualCenter should be installed on a dedicated physical server or virtual machine, since running multiple applications on a VirtualCenter server poses an availability risk. Application programs such as web servers, databases, or messaging systems require a significant number of installed programs, active processes, and privileged users defined. These applications may provide a simple means by which a privileged user unintentionally introduces malicious code. Therefore, VirtualCenter servers will only run those necessary applications that are required to run the VirtualCenter service.

**Computing Check:** On the VirtualCenter Server perform the following.

1. Go to Start>Programs>VMware
2. All VirtualCenter components should be listed under the VMware directory. The VMware Infrastructure Management default installation includes the following components:
  - VMware VirtualCenter Server – A Windows service to manage ESX Server hosts.
  - VI Client – A client application used to connect directly to an ESX Server or indirectly to an ESX Server through a VirtualCenter Server.
  - Microsoft.NET Framework – Software that the VirtualCenter Server, the Database Upgrade wizard, and VI Client users.
  - Microsoft or Oracle Database
  - VMware license server – A Windows service allowing all VMware products to be licensed from a central pool and managed from one console.
  - VMware Update Manager (Optional) – A VirtualCenter plugin that provides security monitoring and patching support for ESX Server hosts and virtual machines.
  - VMware Converter Enterprise for VirtualCenter (Optional) – A VirtualCenter plugin that enables the conversion of physical machines to virtual machines.
3. Next go to Start> Programs>
4. Review all the programs listed to ensure no email servers, office programs, messaging programs, etc. are installed. If so ask the IAO/SA what they are for. If they are unrelated to the VirtualCenter Server, then this is a finding.

**Fix:** Run only the necessary applications for VirtualCenter.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0610:** Patches and security updates are not current on the VirtualCenter Server.

**Vulnerability Key:** V0015860

**STIG ID:** ESX0610

**Vulnerability:** Patches and security updates are not current on the VirtualCenter Server.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 3.1 Patches, 3.2 Operational / PM Patches

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Organizations need to stay current with all applicable VirtualCenter Server software updates that are released from VMware. If updates and patches are not installed, then security vulnerabilities may be open. Open vulnerabilities may provide an access point for an attacker to use to gain access to the system.

**Computing Check:** Go to the VirtualCenter Server and perform the following.

1. Login to the VirtualCenter Server with the VI Client.
2. At the top of the menu select Help>About Virtual Infrastructure.  
The window will appear similar to the figure below.



3. Review the Virtual Infrastructure Version and Build number and compare it the latest patches listed below. If Internet access is available, the reviewer should check for the latest patches on VMware's website to verify the VirtualCenter patches have not been updated recently. The website location is <http://www.vmware.com/download/vi/>. If the version build number is older than the listed ones below, then this is a finding. If the version is not listed or is older than version 2.0.1, then this is a finding as well.

#### VMware VirtualCenter 2.5

Latest Version: 2.5 | 12/10/2007 | Build: 64201

#### VMware VirtualCenter 2.0.2 Update 3

Version: 2.0.2 Update 3 | 2/15/2008 | Build: 75762

#### VMware VirtualCenter 2.0.2 Update 2

Version: 2.0.2 Update 2 | 11/8/2007 | Build: 62327

#### VMware VirtualCenter 2.0.2 Update 1

Version: 2.0.2 Update 1 | 10/29/2007 | Build: 61426 – End of support 11/08/2008

#### VMware VirtualCenter 2.0.2

Version: 2.0.2 | 7/19/2007 | Build: 50618 – End of support 10/29/2008

#### VMware VirtualCenter 2.0.1

Version: 2.0.1 | 10/02/2006 | Build: 32042 – End of support 7/19/2008

**Fix:** Apply all the latest patches to VirtualCenter.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**NOTE:** Checks 650 through 700 only apply if VirtualCenter is installed on a virtual machine. If it is not, then mark all these checks Not Applicable.

**ESX0650:** VirtualCenter virtual machine is not configured in an ESX Server cluster with High Availability

**Vulnerability Key:** V0015864

**STIG ID:** ESX0650

**Vulnerability:** VirtualCenter virtual machine is not configured in an ESX Server cluster with High Availability enabled.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 13.5 Redundancy

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** If the ESX Server hosting the VirtualCenter virtual machine fails, the single point of central administration to the entire virtual infrastructure is gone. To mitigate this potential scenario, High Availability (HA) will be configured through VMware HA. If one ESX Server host fails within a VMware HA cluster, another ESX Server will restart the VirtualCenter virtual machine.

**Computing Check:**

1. Log into the VirtualCenter Server with the VI Client.
2. Verify that there is a cluster configured by reviewing the inventory panel. If no clusters are configured, then this is a finding.
3. Select the cluster and choose Edit Settings from the right-click menu.
4. In the Cluster Settings dialog box, verify Enable VMware HA is selected. If it is not selected, then this is a finding.

**Fix:** Enable High Availability on ESX Server clusters for all VirtualCenter virtual machines.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0660:** VirtualCenter virtual machine does not have a CPU reservation

**Vulnerability Key:** V0015865

**STIG ID:** ESX0660

**Vulnerability:** VirtualCenter virtual machine does not have a CPU reservation.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

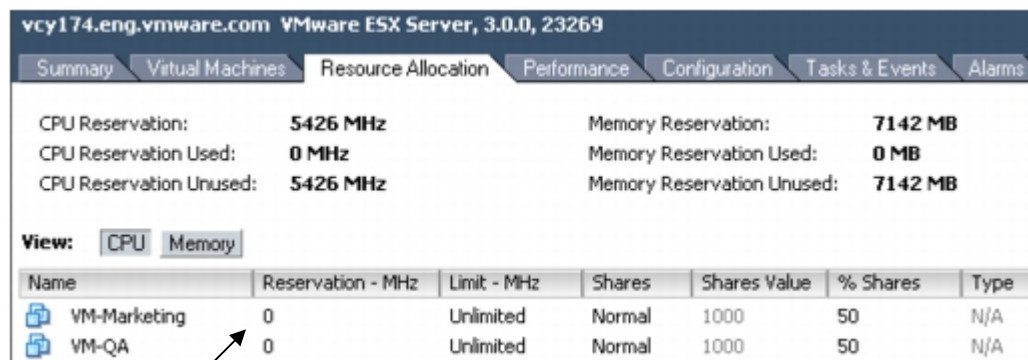
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machine settings affect the availability of the VirtualCenter virtual machine as well. If the virtual machine is not configured with resource reservations, there is no guarantee that the resources will be available.

### Computing Check:

1. Log into VirtualCenter with the VI Client.
  2. In the Inventory panel on the left, select the host that has the VirtualCenter virtual machine.
  3. Select the Resource Allocation Tab and view the reservation for the virtual machine CPU.
- Under View: Select CPU.



vcy174.eng.vmware.com VMware ESX Server, 3.0.0, 23269						
Summary Virtual Machines Resource Allocation Performance Configuration Tasks & Events Alarms						
CPU Reservation:		5426 MHz		Memory Reservation:		7142 MB
CPU Reservation Used:		0 MHz		Memory Reservation Used:		0 MB
CPU Reservation Unused:		5426 MHz		Memory Reservation Unused:		7142 MB
View: CPU Memory						
Name	Reservation - MHz	Limit - MHz	Shares	Shares Value	% Shares	Type
VM-Marketing	0	Unlimited	Normal	1000	50	N/A
VM-QA	0	Unlimited	Normal	1000	50	N/A

Reservation for CPU

4. If the virtual machine reservation says 0, then this is a finding.

**Fix:** Reserve CPU resources for the VirtualCenter virtual machine.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0670:** VirtualCenter virtual machine does not have a Memory reservation

**Vulnerability Key:** V0015866

**STIG ID:** ESX0670

**Vulnerability:** VirtualCenter virtual machine does not have a Memory reservation.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

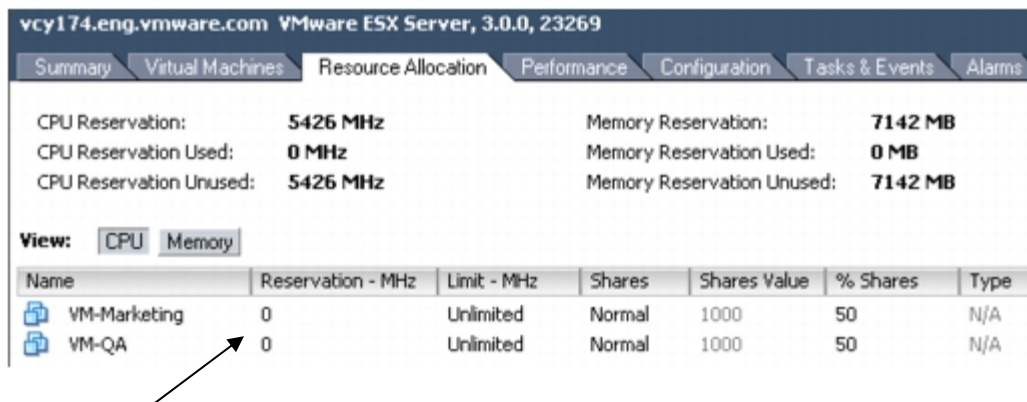
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machine settings affect the availability of the VirtualCenter virtual machine as well. If the virtual machine is not configured with resource reservations, there is no guarantee that the resources will be available.

**Computing Check:**

1. Log into VirtualCenter with the VI Client.
2. In the Inventory panel on the left, select the host that has the VirtualCenter virtual machine.
3. Select the Resource Allocation Tab and view the reservation for the virtual machine Memory. Under View: Select Memory.



vcy174.eng.vmware.com VMware ESX Server, 3.0.0, 23269

Summary Virtual Machines Resource Allocation Performance Configuration Tasks & Events Alarms

CPU Reservation: 5426 MHz Memory Reservation: 7142 MB  
 CPU Reservation Used: 0 MHz Memory Reservation Used: 0 MB  
 CPU Reservation Unused: 5426 MHz Memory Reservation Unused: 7142 MB

View: CPU Memory

Name	Reservation - MHz	Limit - MHz	Shares	Shares Value	% Shares	Type
VM-Marketing	0	Unlimited	Normal	1000	50	N/A
VM-QA	0	Unlimited	Normal	1000	50	N/A

Reservation for Memory

4. If the virtual machine reservation says 0, then this is a finding.

**Fix:** Reserve Memory resources for the VirtualCenter virtual machine.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0680:** CPU alarm is not configured

**Vulnerability Key:** V0015867

**STIG ID:** ESX0680

**Vulnerability:** VirtualCenter virtual machine CPU alarm is not configured.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** To ensure that system administrators are notified if there is a resource problem on the VirtualCenter virtual machine, alarms should be configured to email the administrator. If alarms are not configured, system administrators will not be aware of any resource issues. If resources are unavailable on the VirtualCenter virtual machine, scheduled

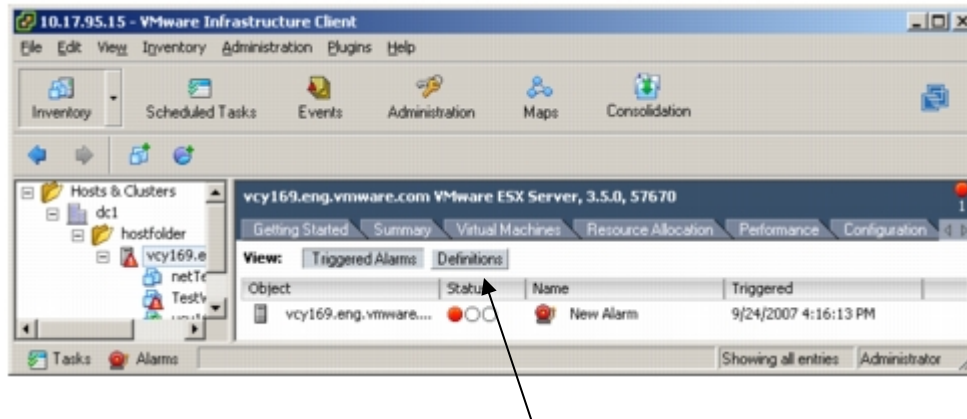


tasks may not be performed, and the potential denial of service on the VirtualCenter virtual machine.

### Computing Check:

1. Log into VirtualCenter with the VI Client.
2. In the Inventory panel on the left, select the host that has the VirtualCenter virtual machine.
3. Click the Alarms tab.
4. To view alarms that have been defined, click Definitions.

A list of defined alarms appears. Double click an alarm definition to display Alarm settings dialog box and view.



Definition

If no Alarm exists that notifies the administrator when the VirtualCenter virtual machine CPU hits 90%, then this is a finding.

**Fix:** Configure an alarm to notify the administrator when the VirtualCenter CPU hits 90%.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0690:** Memory alarm is not configured

**Vulnerability Key:** V0015868

**STIG ID:** ESX0690

**Vulnerability:** VirtualCenter virtual machine Memory alarm is not configured.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

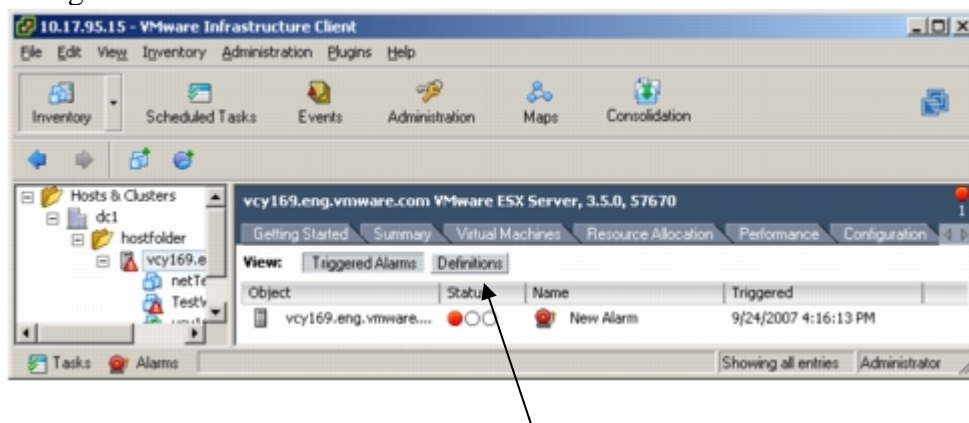
**Severity:** Category III

**Vulnerability Discussion:** To ensure that system administrators are notified if there is a resource problem on the VirtualCenter virtual machine, alarms should be configured to email the administrator. If alarms are not configured, system administrators will not be aware of any resource issues. If resources are unavailable on the VirtualCenter virtual machine, scheduled tasks may not be performed, and the potential denial of service on the VirtualCenter virtual machine.

**Computing Check:**

1. Log into VirtualCenter with the VI Client.
2. In the Inventory panel on the left, select the host that has the VirtualCenter virtual machine.
3. Click the Alarms tab.
4. To view alarms that have been defined, click Definitions.

A list of defined alarms appears. Double click an alarm definition to display Alarm settings dialog box and view.



Definition

If no Alarm exists that notifies the administrator when the VirtualCenter virtual machine Memory hits 90%, then this is a finding.

**Fix:** Configure an alarm to notify the administrator when the VirtualCenter Memory hits 90%.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0700:** Unauthorized users have access to VirtualCenter virtual machine

**Vulnerability Key:** V0015869

**STIG ID:** ESX0700

**Vulnerability:** Unauthorized users have access to the VirtualCenter virtual machine.

**IA Controls:** ECCD-1, ECCD-2 Changes to Data, ECAN-1 Access to Need to Know

**Categories:** 2.1 Object Permissions

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines may be accessed by anyone with the proper permissions. If the VirtualCenter virtual machine is accessed by a normal virtual machine user, specific settings in the virtual infrastructure may be changed or modified. Modifications may include permissions, object groupings, installing malicious software, etc. To mitigate this, access to the VirtualCenter virtual machine will be restricted to only authorized users.

**Computing Check:**

1. Request a copy of the authorized VirtualCenter administrator user documentation. If no documentation exists, then this is a finding.
2. Log into the VI Client as a user with Administrator privileges. Work with the system administrator to access the system with these privileges.
3. In the Inventory panel on the left, select the VirtualCenter virtual machine.
4. Click the Permissions tab.
5. Review the permissions and verify that they match the documentation provided. If there is a discrepancy, then this is a finding.

**Fix:** Restrict access to the VirtualCenter virtual machine to only authorized users.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0710:** No dedicated VirtualCenter administrator created within the Windows Administrator Group

**Vulnerability Key:** V0015870

**STIG ID:** ESX0710

**Vulnerability:** No dedicated VirtualCenter administrator created within the Windows Administrator Group on the Windows Server for managing the VirtualCenter environment.

**IA Controls:** ECCD-1 Changes to Data, ECCD-2 Changes to Data

**Categories:** 2.2. Least Privilege

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** By default, the local administrator or domain administrator is allowed to log on to VirtualCenter. These administrators are allowed since VirtualCenter requires a user with local administrator privileges to run. To limit the local administrative access, a dedicated VirtualCenter account will be created. This VirtualCenter account is an ordinary user that is a member of the local administrators group. This configuration avoids automatically giving administrative access to domain administrators, who typically belong to the local administrators group. This also provides a way of getting into VirtualCenter when the domain controller is down, because the local VirtualCenter administrator account does not require remote authentication.

**Computing Check:**

1. On the VirtualCenter Server, go to Start>Administrative Tools>Computer Management>Local Users and Groups>Groups
2. Open the Administrators group.
3. Verify that a VirtualCenter administrator is listed. Work with the system administrator to identify the user.

If no VirtualCenter administrator is listed, then this is a finding.

**Fix:** Create a VirtualCenter administrator user in the Windows Administrator Group.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0720:** No logon banner warning is configured

**Vulnerability Key:** V0015871

**STIG ID:** ESX0720

**Vulnerability:** No logon warning banner is configured for VirtualCenter users.

**IA Controls:** ECWM-1 Warning Message

**Categories:** 11.6 Warning Banners

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Once users are authenticated by VirtualCenter, users should be presented with a warning message. Presenting a warning message prior to user logon may assist the prosecution of trespassers on the computer system. Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring.

**Computing Check:**

1. Log into VirtualCenter with the VI Client.
2. Select the Administration Menu at the top of the page.
3. Select the Edit Message of the Day.
4. Review the contents and verify the following are listed:  
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC, monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests-not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

If the banner does not contain these items, then this is a finding.

**Fix:** Configure a logon banner in VirtualCenter.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0730:** VI Client sessions with VirtualCenter are unencrypted

**Vulnerability Key:** V0015872

**STIG ID:** ESX0730

**Vulnerability:** VI Client sessions with VirtualCenter are unencrypted.

**IA Controls:** ECCT-1, ECCT-2 Encryption of Transmitted Data

**Categories:** 8.1 Encrypted Data in Transit

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** User sessions with VirtualCenter should be encrypted since transmitting data in plaintext may be viewed as it travels through the network. User sessions may be initiated from the VI client and VI Web Access. To encrypt session data, the sending component, such as a gateway or redirector, applies ciphers to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. To ensure the protection of the data transmitted to and from external network connections, all VI client and web access sessions with VirtualCenter will be encrypted with a FIPS 140-2 encryption algorithm.

**Computing Check:**

1. On the VirtualCenter Server go to Start> Program Files>VMware>Infrastructure>Virtual Infrastructure Client>Launcher.
2. Open the VpxClient.exe.config file with Notepad.
3. Verify https:443 is configured.

```
<appSettings>  
<add key = "protocolports" value = "https:443"/>  
</appSettings>
```

If this setting is not set, then this is a finding.

**Fix:** Encrypt all VI Client sessions to the VirtualCenter Server.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0740:** VI Web Access sessions with VirtualCenter are unencrypted

**Vulnerability Key:** V0015873

**STIG ID:** ESX0740

**Vulnerability:** VI Web Access sessions with VirtualCenter are unencrypted.

**IA Controls:** ECCT-1, ECCT-2 Encryption of Transmitted Data

**Categories:** 8.1 Encrypted Data in Transit

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** User sessions with VirtualCenter should be encrypted since transmitting data in plaintext may be viewed as it travels through the network. User sessions may be initiated from the VI client and VI Web Access. To encrypt session data, the sending component, such as a gateway or redirector, applies ciphers to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. To ensure the protection of the data transmitted to and from external network connections, all VI client and web access sessions with VirtualCenter will be encrypted with a FIPS 140-2 encryption algorithm.

**Computing Check:**

1. Login to VirtualCenter through the VI Client.
2. Select an ESX Server host from the inventory panel.
3. Select the configuration tab.
4. Select advanced settings in the software section.
5. Verify the “Config.Defaults.security.host.ruissl” is checked. This requires SSL to be used when communicating with the host over 902. If this is not checked, then this is a finding.

**Fix:** Encrypt all VI Web Access sessions with VirtualCenter.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0750:** VirtualCenter vpxuser has been modified

**Vulnerability Key:** V0015874

**STIG ID:** ESX0750

**Vulnerability:** VirtualCenter vpxuser has been modified.

**IA Controls:** ECCD-1 Changes to Data, ECCD-2 Changes to Data

**Categories:** 2.1 Object Permissions

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category I

**Vulnerability Discussion:** The vpxuser is created when the ESX Server host is attached to VirtualCenter. It is not present on the ESX Server host unless the host is being managed through VirtualCenter. SAs will not change vpxuser and its default permissions. Modifying these permissions may create problems working with the ESX Server host through VirtualCenter.

**Computing Check:** On the ESX Server service console perform the following:

```
#cd /etc/
```

```
#less passwd | grep vpx
```

Output should appear as follows:

```
vpxuser:x:500:100:Vmware VirtualCenter administration account: /home/vpxuser:/bin/false
```



#less shadow | grep vpx

Output should appear as follows:

vpxuser:(hash value)/:13995:1:360:14::: (These numbers may be different based on the site)

If any of these files have been changed from the above values for the vpxuser, then this is a finding.

**Fix:** Do not modify the vpxuser account.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0760:** Users assigned to VirtualCenter groups are not documented

**Vulnerability Key:** V0015875

**STIG ID:** ESX0760

**Vulnerability:** Users assigned to VirtualCenter groups are not documented.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Ensuring privileged group membership is controlled requires updates to group documentation, and periodic reviews to determine that unauthorized users are not members. If an unauthorized user is able to gain membership to the Database Administrator group, Virtual Machine Administrator group, or the Resource Administrator group, etc., that user would be able to display, add, or change permissions to objects that could impact the confidentiality, integrity, or availability of an entire virtualization structure.

**Non-Computing Check:** Request a copy of the VirtualCenter group documentation listing the following users in the following groups:

Database Administrators

Virtual Machine Administrators  
Resource Pool Administrators  
ESX Administrators  
Virtual Machine Power Users  
All Custom Roles

If no documentation can be produced, then this is a finding. Compare the documentation to the actual users assigned in the groups. If there are discrepancies, then this is a finding.

**Fix:** Document all the users assigned to all VirtualCenter groups.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0770:** Users are not documented in the Windows Administrators group

**Vulnerability Key:** V0015876

**STIG ID:** ESX0770

**Vulnerability:** Users are not documented that are in the VirtualCenter Server Windows Administrators group.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Users who are members of the Windows administrators group on the VirtualCenter server are granted the same access rights as any user assigned to the VirtualCenter administrator role. These users need to be documented to ensure only authorized users are members of this group.

**Non-Computing Check:** Request a copy of the users assigned to the Windows Administrators group on the VirtualCenter Server. If no documentation exists, then this is a finding. Compare

the documented users to those listed in the group on the server. If any discrepancies exist, then this is a finding.

**Fix:** Document all users in the Windows Administrators group.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0780:** VirtualCenter Server groups are not reviewed monthly

**Vulnerability Key:** V0015877

**STIG ID:** ESX0780

**Vulnerability:** VirtualCenter Server groups are not reviewed monthly.

**IA Controls:** ECAT-1 Audit, Trail, Monitoring, Analysis, and Reporting, ECAT-2 Audit, Trail, Monitoring, Analysis, and Reporting

**Categories:** 10.3 Review

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Reviewing the VirtualCenter groups will ensure that no unauthorized users have been granted access to objects.

**Non-Computing Check:** Ask the IAO/SA how often the following groups are reviewed on the VirtualCenter Server.

Windows Administrators group  
Database Administrators  
Virtual Machine Administrators  
Resource Pool Administrators  
ESX Administrators  
Virtual Machine Power Users  
All Custom Roles

If these groups are not reviewed at least monthly, then this is a finding.

**Fix:** Review the VirtualCenter groups monthly.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0790:** No documented configuration management process exists for VirtualCenter changes

**Vulnerability Key:** V0015878

**STIG ID:** ESX0790

**Vulnerability:** No documented configuration management process exists for VirtualCenter changes.

**IA Controls:** DCPR-1 Configuration Management Process

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** VirtualCenter objects might have multiple permissions for users and or groups. Permissions are applied hierarchically downward on these objects. For each permission the administrator must decide if the permission applies only to that immediate object, or downward to all sub objects. Permissions may be overridden by setting different permissions on a lower object. These situations can create confusion and permissions that were thought to be limited might actually be elevated. Furthermore, all changes take affect immediately not requiring users to log off and log back in. Configuration management is critical for all modifications since the new change may override previously configured permissions.

**Non-Computing Check:** Request a copy of the configuration management process document. If the document is incomplete or does not exist, then this is a finding.

**Fix:** Document a configuration management process for all VirtualCenter modifications.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0800:** There is no VirtualCenter baseline configuration document

**Vulnerability Key:** V0015879

**STIG ID:** ESX0800

**Vulnerability:** There is no VirtualCenter baseline configuration document for users, groups, permissions, and roles.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** When pairing users or groups with permissions to an object, a role is defined for users and groups. There are two default roles defined in VirtualCenter called System roles and Sample roles. System roles are permanent and the permissions associated with these roles cannot be changed. Sample roles are provided for convenience as guidelines and suggestions. These roles may be modified or removed. VirtualCenter situations may arise where a user is a member of multiple groups with different permissions or user permissions are explicitly defined when the user is a member of different groups.

These situations can create confusion and permissions that were thought to be limited might actually be elevated. Furthermore, all changes take affect immediately not requiring users to log off and log back in. Therefore, all users, groups, permissions, and roles will be documented and approved to ensure proper permissions are granted only to authorized users.

**Non-Computing Check:** Request a copy of the baseline configuration document for all VirtualCenter users, groups, permissions, and roles. If the document is incomplete or does not exist, then this is a finding.

**Fix:** Create a baseline configuration document for all VirtualCenter users, groups, permissions, and roles.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0810:** VirtualCenter does not log user, group, permission, or role changes

**Vulnerability Key:** V0015880

**STIG ID:** ESX0810

**Vulnerability:** VirtualCenter does not log user, group, permission or role changes.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record Retention

**Categories:** 10.4 Reporting

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** VirtualCenter Servers not configured to log user, group, permission and role changes will not have the ability to review past system and user events. Recording these events is critical to establishing a recorded history of system events, enabling system administrators to diagnose intermittent system problems, suspicious user activity, and assisting with investigations. Log events also verify that the established policies configured on the system are in fact working as configured.

**Computing Check:**

1. Log into VirtualCenter with the VI Client.
2. Select the Administration Menu at the top of the page.
3. Select VirtualCenter Management Server Configuration.
4. Select Logging Options.
5. Verify that VirtualCenter Logging is configured to Info(Normal Logging) or higher (Verbose or Trivia)

**Fix:** Configure VirtualCenter Logging to Info or higher.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0820:** VirtualCenter logs are not reviewed daily

**Vulnerability Key:** V0015881

**STIG ID:** ESX0820

**Vulnerability:** VirtualCenter logs are reviewed daily.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** It is necessary to review VirtualCenter logs or suspicious activity, problems, attacks, or system warnings will go undetected. These logs provide visibility into the activities and events of the VirtualCenter. These logs enable system administrators and auditors the ability to recreate past events, monitor the system, and ensure security policies are being enforced.

**Non-Computing Check:** Ask the IAO/SA how often they review the VirtualCenter logs. VirtualCenter logs include System Logs and Events. If the logs are not reviewed daily, then this is a finding.

**Fix:** Review the VirtualCenter logs daily.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0860:** There is no up-to-date documentation of the virtualization infrastructure

**Vulnerability Key:** V0015882

**STIG ID:** ESX0860

**Vulnerability:** There is no up-to-date documentation of the virtualization infrastructure.

**IA Controls:** DCHW-1 Baseline Hardware Inventory, DCSW-1 Baseline Software Inventory

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** With the creation of virtual machines, the actual virtual network topology becomes increasingly complex. The topology changes when a virtual machine is created, added to a virtual switch or port group, moved to another virtualization server, etc. With the dynamic nature of the virtualization environment, administrators of the virtualization environment will maintain up to date documentation for all virtual machines, virtual switches, IP addresses, MAC addresses, etc.

**Non-Computing Check:** Request a copy of all the virtualization infrastructure documentation. Documentation must include all ESX Servers, virtual machines, IP addresses, MAC addresses, virtual switches, operating systems, and any virtual applications. If the documentation does include all of these components, then this is a finding.

**Fix:** Develop up-to-date documentation for the virtualization infrastructure.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0863:** ESX Server is not properly registered in VMS

**Vulnerability Key:** V0015973

**STIG ID:** ESX0863

**Vulnerability:** ESX Server is not properly registered in VMS.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 12.4 CM Process



**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Running the most current, approved version of software on all ESX Servers will help maintain a stable base of security fixes as well as security enhancements. ESX Servers that are not running the latest tested and approved versions of software are vulnerable to the potential attacks. Furthermore, if the ESX Server is no longer supported by the vendor, patches will not be made available to address weaknesses exposing new vulnerabilities, nor will IAVM notices be made available that provide announcements of these new vulnerabilities along with measures to mitigate their associated risks.

**Computing Check:** Use VMS and navigate to the site's assets. Ensure the ESX Server(s) are registered within VMS. If they are not registered, this is a finding.

**Fix:** Register ESX Servers in VMS.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0866:** ESX Server assets are not configured with the correct posture in VMS.

**Vulnerability Key:** V0015974

**STIG ID:** ESX0866

**Vulnerability:** ESX Server assets are not configured with the correct posture in VMS.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Correctly configuring the ESX Server asset in VMS will ensure that the appropriate vulnerabilities are assigned to the asset. If the asset is not configured with the

correct posture, vulnerabilities may be open on the asset. These open vulnerabilities may allow an attacker to access the system.

**Computing Check:** If check ESX0863 is a finding, this should be marked a finding also.

If the assets are registered, verify that the following postures are registered. If any of the postures are not registered this is a finding.

ESX Server 3  
Tomcat 5.x

**Fix:** Register ESX Servers in VMS with the correct posture.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0869:** VirtualCenter Server assets are not properly registered in VMS

**Vulnerability Key:** V0015975

**STIG ID:** ESX0869

**Vulnerability:** VirtualCenter Server assets are not properly registered in VMS.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Running the most current, approved version of software on all VirtualCenter Servers will help maintain a stable base of security fixes as well as security enhancements. VirtualCenter Servers that are not running the latest tested and approved versions of software are vulnerable to the potential attacks. Furthermore, if the VirtualCenter Server is no longer supported by the vendor, patches will not be made available to address weaknesses exposing new vulnerabilities, nor will IAVM notices be made available that provide announcements of these new vulnerabilities along with measures to mitigate their associated risks.

**Computing Check:** Use VMS and navigate to the site's assets. Ensure the VirtualCenter Server(s) are registered within VMS. If they are not registered, this is a finding.

**Fix:** Register VirtualCenter Servers in VMS.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0872:** VirtualCenter Server assets are not configured with the correct posture in VMS.

**Vulnerability Key:** V0015984

**STIG ID:** ESX0872

**Vulnerability:** VirtualCenter Server assets are not configured with the correct posture in VMS.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Correctly configuring the VirtualCenter Server asset in VMS will ensure that the appropriate vulnerabilities are assigned to the asset. If the asset is not configured with the correct posture, vulnerabilities may be open on the asset. These open vulnerabilities may allow an attacker to access the system.

**Computing Check:** If check ESX0869 is a finding, this should be marked a finding also.

If the assets are registered, verify that the following postures are registered. The database may be SQL or Oracle. Use the appropriate database entry when applying the posture for the database. If any of the postures are not registered this is a finding. For instance, the SQL Server 2005 posture will look as follows:

- Win2k3
- Database SQL Server Installation 2005
- Database SQL Server Database 2005 – Model
- Database SQL Server Database 2005 – Master
- Database SQL Server Database 2005 – MSDB

Database SQL Server Database 2005 – TempDB  
Database SQL Server Database 2005 – VCDB  
Antivirus  
Tomcat 5.x

**Fix:** Register VirtualCenter Server with the correct posture in VMS.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

### 3. VIRTUAL MACHINE ADMINISTRATOR CHECKLIST

The Virtual Machine Administrator role is responsible for creating and configuring virtual machines, virtual networks, virtual machine resources, and security policies. The Virtual Machine Administrator creates, maintains, and provisions virtual machines, and virtual networks through VirtualCenter.

**ESX0880:** ISO images are not restricted to authorized users

**Vulnerability Key:** V0015884

**STIG ID:** ESX0880

**Vulnerability:** ISO images are not restricted to authorized users.

**IA Controls:** ECCD-1, ECCD-2 Changes to Data, ECAN-1 Access to Need to Know

**Categories:** 2.1 Object Permissions

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines are created from using operating system CD-ROMs or ISO images of the operating system. ISO operating system images reduce the time in deploying virtual machine servers since the media is readily available as a file on the hard drive. Also, ISO operating system images map easily to the virtual machine CD-ROM drive of the guest machine once the guest machine is running. Unauthorized access to the ISO operating system images could potentially allow these images to be corrupted or altered in some way.

**Computing Check:**

On the ESX Server service console perform the following command to determine if the /ISO, /Utilities, or /Images file partitions are accessible to unauthorized users.

```
# ls -la /(the name of the partition)/(name of image).iso
```

If any of the /(the name of the partition)/(name of image) files are readable by unprivileged id's, then this is a finding. The only users that should have access to these are root.

**Fix:** Restrict iso images to only authorized users.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0890:** ISO images do not have hash checksums

**Vulnerability Key:** V0015885

**STIG ID:** ESX0890

**Vulnerability:** ISO images do not have hash checksums.

**IA Controls:** ECTM-1, ECTM-2 Transmission Integrity Controls, DCNR-1 Non-Repudiation

**Categories:** 8.5 Hashing

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Since ISO operating system images are typically large files, transferring these ISO operating system images over the network may cause corruption to the files. There are simple ways to check the integrity of the file on both the source and destination system using hashing algorithms. Users should create hash checksums on all ISO operating system images on the ESX Server before utilizing the ISO operating system image for virtual machines.

**Computing Check:**

On the ESX Server service console go to the partition that stores the ISO images and verify hash checksums are present for any ISO files. Perform the following to determine if ISO images are verified for integrity:

```
#cd /(ISO partition)
#cat sha1sum
```

If no sha1sums are returned or the number of ISO images is different from the number of sha1sums, then this is a finding.

**Fix:** Create SHA1 checksums for all ISO images.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0900:** ISO images are not verified for integrity

**Vulnerability Key:** V0015886

**STIG ID:** ESX0900

**Vulnerability:** ISO images are not verified for integrity when moved across the network.

**IA Controls:** ECTM-1, ECTM-2 Transmission Integrity Controls, DCNR-1 Non-Repudiation

**Categories:** 8.5 Hashing

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Since ISO operating system images are typically large files, transferring these ISO operating system images over the network may cause corruption to the files. There are simple ways to check the integrity of the file on both the source and destination system using hashing algorithms. Users should create hash checksums on all ISO operating system images on the ESX Server before utilizing the ISO operating system image for virtual machines.

#### **Computing Check:**

On the ESX Server service console go to the partition that stores the ISO images and verify hash checksums are present for any ISO files. Perform the following to determine if ISO images are verified for integrity:

```
#cd /(ISO partition)
#cat sha1sum
```

#sha1sum (ISO image) - Pick an ISO image to test

Compare the sha1sum against each other to ensure they are the same. If they are not the same, then this is a finding.

**Fix:** Verify all SHA1 checksums for all ISO images.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0910:** Master templates are not stored on a separate partition

**Vulnerability Key:** V0015887

**STIG ID:** ESX0910

**Vulnerability:** Master templates are not stored on a separate partition.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** The master templates will be stored in a separate partition (NTFS, VMFS, etc) from the production virtual machines. Partitioning the master templates isolates them from system, application, and user files. This isolation helps protect the disk space used by the operating system and various applications. Files cannot grow across partitions. Another advantage is that if a bad spot develops on the hard drive, the risk to the data is reduced as is recovery time. Furthermore, separate master template partitions provide the ability to set up certain directories as read-only file systems.

**Computing Check:**

Perform the following on the ESX Server service console to determine if the /Master, /Utilities, /Images, or /(the name of the partition) are on separate disk partitions:

#vdf -h

Examine the Mounted on column for the disk device and ensure the device label for /Master, /Utilities, or /Images is not the same as the root filesystem. If they are the same, then this is a finding.

**Fix:** Store all master templates on a separate partition.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0920:** Master templates are not restricted to authorized users only

**Vulnerability Key:** V0015888

**STIG ID:** ESX0920

**Vulnerability:** Master templates are not restricted to authorized users only.

**IA Controls:** ECCD-1, ECCD-2 Changes to Data, ECAN-1 Access to Need to Know

**Categories:** 2.1 Object Permissions

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Restricting access to master templates to authorized users helps ensure they are not compromised or modified. If these master templates were compromised, all future guest installations could be corrupt or contain malicious code. Master templates will be restricted to only users that are administering and/or creating guest virtual machines.

**Computing Check:**

On the ESX Server service console perform the following command to determine if the /Master, /Utilities, or /Images file partitions are accessible to unauthorized users.

```
# ls -la /(the name of the partition)/(name of master template)
```

If any of the /(the name of the partition)/(name of master template) files are readable by unprivileged id's, then this is a finding. The only users that should have access to these are root.

**Fix:** Restrict master templates to authorized users only.



Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0930:** The VMware-converter utility is not used for VMDK imports or exports

**Vulnerability Key:** V0015889

**STIG ID:** ESX0930

**Vulnerability:** The VMware-converter utility is not used for VMDK imports or exports.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** There will be situations that require the import or export of VMDK files on the VMFS partition. Importing and exporting disk files can also be done through the Virtual Infrastructure Client or service console by copying the files from VMFS mount and pasting them to a partition running ext3 file system. Utilizing the VMware-converter utility is required since the VMFS file system utilizes such large files. There are third-party converters available that may work with VMware virtual machines, however, none have been thoroughly tested or approved by VMware.

**Non-Computing Check:** Ask the IAO/SA how they import and export VMDK files. If they are using the VMware-converter utility, then this is not a finding. If they are using a third party converter, ensure that the converter is supported by the vendor. This might require going to the vendor's website and verifying the version used is supported. If it is not, then this is a finding.

**Fix:** Use the VMware-converter for all import and export of VMDK files to VMFS partitions.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0940:** Nonpersistent disk mode is not set for virtual machines

**Vulnerability Key:** V0015890

**STIG ID:** ESX0940

**Vulnerability:** Nonpersistent disk mode is not set for virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The security issue with nonpersistent disk mode is that attackers may undo or remove any traces that they were ever on the machine with a simple shutdown or reboot. Once the virtual machine has been shutdown, the vulnerability used to access the virtual machine will still be present, and the attacker may access the virtual machine in the future at a point in time of their choice. The danger is that administrators may never know if they have been attacked or hacked. To safeguard against this, nonpersistent disk mode will be only used for test and development virtual machines. Production virtual machines will be set to persistent disk mode only.

**Computing Check:** Pick one or two virtual machines to verify for compliance.

1. Log into the VirtualCenter Server with the VI Client and select the server from the inventory panel.

The hardware configuration page for the server appears.

2. Expand the inventory as needed, and select the virtual machine that you would like to check.
3. Click the Edit Settings link in the Commands panel to display the Virtual Machine Properties dialog box.
4. Select the Hardware tab.
5. Click the appropriate Hard Disk in Hardware list, and verify that Nonpersistent mode is not selected. If nonpersistent mode is selected, then this is a finding.

**Caveat:** Nonpersistent disk mode may be used if it has been documented and approved by the DAA.

**Fix:** Configure all virtual machines to use persistent disk mode only, which is the default.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0950:** No policy exists to assign virtual machines to personnel

**Vulnerability Key:** V0015891

**STIG ID:** ESX0950

**Vulnerability:** No policy exists to assign virtual machines to personnel.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 2.3 Ownership

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** In traditional computing environments, servers were usually assigned to various personnel for administration. For instance, the data server was administered by the database administrator; the domain controller was maintained by the network administrator, etc. Other methods include assigning the MAC address to specific personnel or identifying machines by Ethernet location or port number. All these approaches are impractical in the virtual machine environment.

In the virtual environment, virtual machines may be moved or have MAC addresses that may change. These scenarios make it difficult to establish who owns the virtual machine running on a particular host. Therefore, a policy will need to be implemented to identify and assign virtual machines to the appropriate personnel.

**Non-Computing Check:** Request a copy of the policy that is used to assign virtual machines to personnel. If no policy or procedure exists, then this is a finding.

**Fix:** Develop a policy for assigning virtual machines to the appropriate personnel.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0960:** VI Console is used to administer virtual machines

**Vulnerability Key:** V0015892

**STIG ID:** ESX0960

**Vulnerability:** VI Console is used to administer virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** The VI Console allows a user to connect to the console of a virtual machine, similar to seeing what a physical server monitor would show. However, the VI Console also provides power management and removable device connectivity controls, which could potentially allow a malicious user to bring down a virtual machine. In addition, it also has a performance impact on the service console, especially if many VI Console sessions are open simultaneously. To prevent performance issues and potential unauthorized users from accessing the VI Console, users should use remote management services, such as terminal services and ssh, to interact with virtual machines.

**Non-Computing Check:** Ask the IAO/SA what tools are used to administer virtual machines remotely. If the response includes the VI console, then this is a finding.

**Fix:** Use third party tools to administer virtual machines.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0970:** Clipboard capabilities are enabled for virtual machines

**Vulnerability Key:** V0015893

**STIG ID:** ESX0970

**Vulnerability:** Clipboard capabilities (copy and paste) are enabled for virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

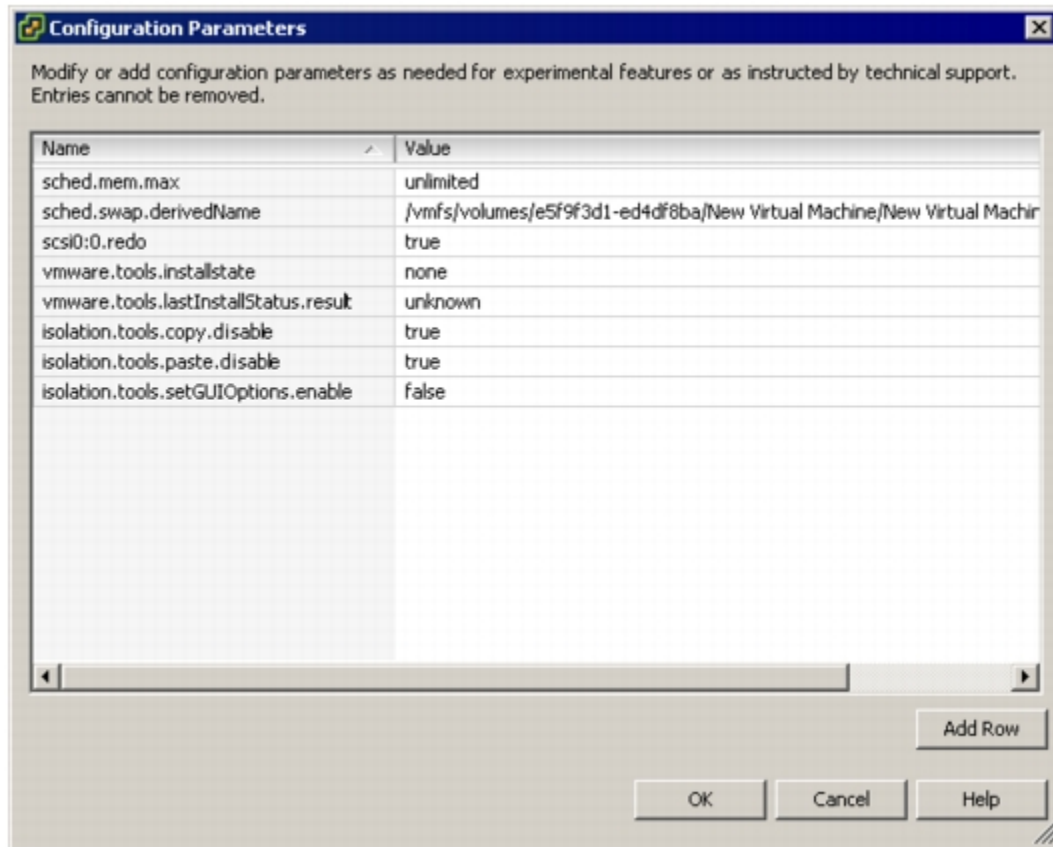
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Several security issues arise with the clipboard. The first is that the system administrator might turn on the clipboard transfer and use it. However, deselecting the clipboard check box will not turn off the function, since a reboot is required. So, the clipboard function is still active. Therefore, transferring text objects, such as a password from one clipboard to another, in any direction between the virtual machine and the host operating system is possible. Secondly, this breaks the virtual machine isolation. This may cause information leakage and potentially infect other operating systems if the text is a string that can be run as a command or URL. As a result of these behaviors, all clipboard capabilities should be disabled within the virtual machine.

**Computing Check:**

1. Login to VirtualCenter with the VI Client and select a virtual machine from the inventory panel.  
The configuration page for the virtual machine appears with the Summary tab displayed.
2. Click Edit Settings.
3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.
4. The result should appear as follows:



If the following settings are not configured, then this is a finding.

Isolation.tools.copy.disable	true
Isolation.tools.paste.disable	true
Isolation tools.setGUIOptions.enable	false

**Fix:** Disable the clipboard capabilities in all virtual machines.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX0980:** VMware Tools drag and drop capabilities are enabled

**Vulnerability Key:** V0015894

**STIG ID:** ESX0980

**Vulnerability:** VMware Tools drag and drop capabilities are enabled for virtual machines.

## **IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The drag and drop operation maybe used to transfer files from the guest virtual machine to the computer connecting to the virtual machine via the VI Console. Files may be moved from the guest virtual machine to the VI Console computer through the drag and drop functionality. This functionality has several potential damaging consequences. The file moved to the VI Console computer may be so large that it fills the hard disk on the system, may contain sensitive information, or may contain malicious code. These scenarios could potentially cause a denial of service to the VI Console computer, expose sensitive information to unauthorized users, or run malicious code.

### **Computing Check:**

1. Login to VirtualCenter with the VI Client and select a virtual machine from the inventory panel.
- The configuration page for the virtual machine appears with the Summary tab displayed.
3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.
4. Verify the following is displayed in the result:

isolation.tools.dnd.disable                      true

If this is not present, then this is a finding.

**Fix:** Disable drag and drop in VMware Tools.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX0990:** The VMware Tools setinfo variable is enabled for virtual machines

.

**Vulnerability Key:** V0015895

**STIG ID:** ESX0990

**Vulnerability:** The VMware Tools setinfo variable is enabled for virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The virtual machine operating system sends informational messages to the ESX Server host through VMware Tools. These messages are setinfo messages and typically contain name-value pairs that define virtual machine characteristics or identifiers that the ESX Server stores. For instance, a setinfo message may be ipaddress=10.10.15.224. A setinfo message has fixed formats and lengths. Therefore, the amount of data passed to the ESX Server this way is limited. However, the data flow provides an opportunity for an attacker to stage a DOS attack by writing software that mimics VMware Tools by flooding the ESX Server with packets, and consuming resources needed by virtual machines. To mitigate this, the virtual machine administrator should disable the setinfo variable. This will prevent the guest operating system processes from sending messages to the ESX Server.

**Computing Check:**

1. Login to VirtualCenter with the VI Client and select a virtual machine from the inventory panel.
- The configuration page for the virtual machine appears with the Summary tab displayed.
3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.
4. The result should appear as follows:



Name	Value
sched.mem.max	unlimited
sched.swap.derivedName	/vmfs/volumes/e5f9f3d1-ed4df8ba/New Virtual Machine/New Virtual Machine-
scsi0:0.redo	true
vmware.tools.installstate	none
vmware.tools.lastInstallStatus.result	unknown
isolation.tools.setinfo.disable	true

If the isolation.tools.setinfo.disable is not configured to true, then this is a finding.

**Fix:** Disable the setinfo variable.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1000:** Configuration tools are enabled for virtual machines

**Vulnerability Key:** V0015896

**STIG ID:** ESX1000

**Vulnerability:** Configuration tools are enabled for virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** There are other settings that should be specified in the configuration files for virtual machines. The connectable setting disables connecting and disconnecting removable devices from within the virtual machine. The diskShrink setting shrinks the virtual disk. The diskWiper defragments virtual disks. These last two settings could effectively DOS the system by having the virtual disk defragmented and shrunk on demand.

The commands that should be disabled are listed:

isolation.device.connectable.disable = "TRUE"

isolation.tools.diskShrink.disable = "TRUE"

isolation.tools.diskWiper.disable = "TRUE"

**Computing Check:**

1. Login to VirtualCenter with the VI Client and select a virtual machine from the inventory panel.

The configuration page for the virtual machine appears with the Summary tab displayed.

3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.

4. Verify the following is displayed in the result:

isolation.device.connectable.disable                      true

isolation.tools.diskShrink.disable                        true

isolation.tools.diskWiper.disable                         true

If these are not configured, then this is a finding.

**Fix:** Disable configuration tools for the virtual machine.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1010:** Virtual machines are not time synchronized

**Vulnerability Key:** V0015897

**STIG ID:** ESX1010

**Vulnerability:** Virtual machines are not time synchronized with the ESX Server or an authoritative time server.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** The accuracy of time within the virtualization environment is difficult due to the timer interrupt issue. Time drifts may be as dramatic as 5-10 minutes. Inaccurate time causes other inaccuracies within the virtualization environment, which may include event logs, domain synchronization, session timeouts, etc. Virtual machine time synchronization may be achieved through an external time source or through the ESX Server operating system.

**Computing Check:**

1. Ask the IAO/SA how virtual machines are time synchronized. If they synchronized to an external server, then go to step 2. If configured to the ESX Server host, then go to step 3.  
2. Time servers are configured in the /etc/ntp.conf file on UNIX systems. Once they are configured with an atomic clock, the ntpd daemon should be configured to start at the runlevels 3, 4, and 5. Windows servers are configured via the command line using the net time /setsntp:clock.isc.org. The w32time service will need to be configured to start after the change.

Unix Systems:

#less /etc/ntp.conf

Verify a valid time server is listed. If not, this is a finding.

Windows systems:

Start, run, cmd

C:\>net time /querysnTP

If no results are displayed to use a valid SNTP server, then this is finding.

3. Login to VirtualCenter with the VI Client and select a virtual machine from the inventory panel.

4. Click the Edit Settings link in the Commands panel.

The Virtual Machine Properties dialog box is displayed. Select the Options tab.

5. Select VMware Tools in the Settings list.

6. Verify the guest operating system is configured to synchronize time with the host ESX Server. This is enabled when the “Synchronize guest time with host” option is checked. If it is not checked, then this is a finding.

**Fix:** Synchronize the virtual machine with an external time source or the ESX Server host.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1020:** The IAO/SA does not document and approve virtual machine renames

**Vulnerability Key:** V0015898

**STIG ID:** ESX1020

**Vulnerability:** The IAO/SA does not document and approve virtual machine renames.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** It may become necessary to rename a virtual machine at some point during the course of testing to production. To rename a virtual machine, the virtual machine must be powered down before proceeding with the renaming feature. It is also practice to backup virtual machines before renaming any virtual machine. The configuration files for VMware are typically located on the service console in /root/VMware/ directory, and the virtual disks will be in the /vmfs/ directory. Renaming virtual machines may cause communication issues on the network with other servers, users, etc. To prevent communication disruptions to the network or virtual machine, all virtual machine renames will be documented and approved by the change control board.

**Non-Computing Check:** Request a copy of the virtual machine rename approval documentation from the IAO/SA. If no documentation can be produced, then this is a finding.

**Fix:** Develop approval documentation for all virtual machine renames.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1030:** Test and development virtual machines are not logically separated from production virtual machines

**Vulnerability Key:** V0015899

**STIG ID:** ESX1030

**Vulnerability:** Test and development virtual machine are not logically separated from production virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Test and development virtual machines will be logically separated from the production virtual machines. Logically separating test and development virtual machines ensures that any test and development traffic does not traverse the production LAN. This traffic separation will enhance the availability of the production servers. The preferred logical configuration is for the test and development VLAN to be assigned a dedicated physical network adapter on the ESX Server. If this is not feasible, then a separate VLAN on the production physical network adapter is acceptable.

**Computing Check:** Ask the IAO/SA if test and development virtual machines are configured on the same ESX Server farm as production virtual machines. If so, then proceed to step 1. Otherwise, this is Not Applicable.

1. Log into VirtualCenter with the VI Client and select the server from the inventory panel.  
The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Examine the virtual switches and their respective VLAN IDs. A separate and dedicated VLAN ID should be configured for test and development virtual machines. If there is no VLAN ID defined for test and development virtual machines, then this is a finding.

**Fix:** Assign a dedicated VLAN ID for all test and development virtual machines.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1040:** No policy exists to restrict copying or sharing virtual machines over networks and removable media

**Vulnerability Key:** V0015900

**STIG ID:** ESX1040

**Vulnerability:** No policy exists to restrict copying and sharing virtual machines over networks and removable media.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** As virtual machines replace real hardware they can undermine the security architecture of many organizations which often assume predictable and controlled change number of hosts, host configurations, host locations etc. Some useful mechanisms that virtual machines provide are copying or sharing virtual machine hard disks. Copying or sharing virtual machine hard disks can be done over networks and removable media. Typically, test and development virtual machines will be moved and updated more frequently than production virtual machines. There will be a policy in place to restrict the copying and sharing of production virtual machines over networks and removable media to ensure that administrators do not give unauthorized users access to the virtual machine files.

**Non-Computing Check:** Request a copy of the policy restricting virtual machine sharing and copying over networks and removable media. If no policy exists, then this is a finding.

**Caveat:** This is not applicable to snapshot backups, disaster recovery virtual machines, test and development virtual machines, and clustered virtual machines.

**Fix:** Develop a policy that prohibits virtual machine sharing and copying over networks and removable media.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1050:** Virtual machine moves are not logged

**Vulnerability Key:** V0015901

**STIG ID:** ESX1050

**Vulnerability:** Virtual machine moves are not logged from one physical server to another.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record

**Categories:** 10.4 Reporting

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines may be moved from one computer to another similar to a normal file. This portability gives rise to a host of security problems. In the virtual machine world, the trusted computing base consists of all the hosts that the virtual machine has run on. If no history was maintained for each virtual machine, this can make it very difficult to figure out how far a security compromise has extended if the virtual machine has been moved several times.

**Computing Check:** Ask the IAO/SA if Vmotion is used to migrate virtual machines from one ESX Server host to another. If not, then this is Not Applicable. If so, then perform the following on the ESX Server service console:

```
#cd /var/log/vmware/vpx  
#grep -in vmotion vpxa*.log
```

If the logs are compressed, then perform the following:

```
#zcat vpxa*.log.gz | grep -i vmotion
```

If no result is returned, then this is a finding.

**Fix:** Log all VMotion migrations.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1060:** Virtual machine moves to removable media are not documented

**Vulnerability Key:** V0015902

**STIG ID:** ESX1060

**Vulnerability:** Virtual machine moves to removable media are not documented.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** From a theft perspective, virtual machines are easy to copy and move to a person's USB drive, portable hard drive, etc. An insider could potentially move the organization's entire data center on any type of removable media that had sufficient space.

**Non-Computing Check:** Ask the IAO/SA if virtual machines have been copied to removable media (DVD, CD-ROM, USB drives). If so, request the documentation for all virtual machine moves to removable media. If no documentation exists, then this is a finding.

**Fix:** Document all virtual machine moves to removable media.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1070:** Virtual machines are removed from the site without approval documentation

**Vulnerability Key:** V0015903

**STIG ID:** ESX1070



**Vulnerability:** Virtual machines are removed from the site without approval documentation.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** From a theft perspective, virtual machines are easy to copy and move to a person's USB drive, portable hard drive, etc. An insider could potentially move the organization's entire data center on any type of removable media that had sufficient space.

**Non-Computing Check:** Request the approval documentation from the IAO/SA that the site uses for all virtual machines taken off site. If no documentation exists, then this is a finding.

**Fix:** Create documentation to use for virtual machines taken off site.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1080:** Production virtual machines are not located in a controlled access area

**Vulnerability Key:** V0015904

**STIG ID:** ESX1080

**Vulnerability:** Production virtual machines are not located in a controlled access area.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 5.11 Controlled Access Area

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines may contain an aggregate of sensitive and non-sensitive data. If this data is not located in a controlled access area, unauthorized users may gain access to the virtual machines and have access to the data. This access may result in the loss of privacy and data theft.

**Computing Check:** Review the location of the virtual machines. Ensure that authorized users are required to verify their identity and authority before gaining access to the virtual machines. If the virtual machines are not located in a controlled access area, then this is a finding.

**Fix:** Place all virtual machines in a controlled access area.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1090:** Virtual machine rollbacks are performed when virtual machine is connected to the network.

**Vulnerability Key:** V0015905

**STIG ID:** ESX1090

**Vulnerability:** Virtual machine rollbacks are performed when virtual machine is connected to the network.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Virtual machines may be rolled back to a previous state. Rolling back a virtual machine can re-expose patched vulnerabilities, re-enable previously disabled accounts or passwords, remove log files of a machine, use previously retired encryption keys, and change firewalls to expose vulnerabilities. Rolling back virtual machines can also reintroduce malicious code, and protocols reusing TCP sequence numbers that had been previously removed, which could allow TCP hijacking attacks.

**Non-Computing Check:** Ask the IAO/SA the process used for virtual machine rollbacks. If no process is used that includes disconnecting the virtual machine from the network before performing a revert to snapshot or rollback, then this is a finding.

**Fix:** Disconnect from the network or power off the virtual machine before rollbacks.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1100:** Virtual machine OS log files are not saved before rollback

**Vulnerability Key:** V0015906

**STIG ID:** ESX1100

**Vulnerability:** Virtual machine OS log files are not saved before rollback.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record Retention

**Categories:** 10.5 Retention

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Traditionally, a physical server's lifetime can be envisioned as a straight line where the current state of the machine is a static point forward as software executes, configuration changes made, and software is installed. In a virtual environment the virtual machine state is more akin to a tree, where at any point the execution can fork of into  $N$  different branches. These different branches are the multiple instances of the virtual machine running or existing at any point in time. Branches are caused by taking multiple snapshots in a continuous manner. These multiple virtual machines may be rolled back to previous states in their execution and activity that was once logged maybe lost if the log files are not archived before the rollback.

**Computing Check:** Typically the OS log files are sent to a syslog server. Ask the IAO/SA the location of all archived OS logs that were saved before any rollback or revert to snapshot of the virtual machine. Correlate the logs to the rollback time to ensure that they are legitimate. If no logs have been saved, then this is a finding.

**Fix:** Archive all virtual machine OS log files before any virtual machine rollback.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1110:** Virtual machine log files do not have a size limit

**Vulnerability Key:** V0015907

**STIG ID:** ESX1110

**Vulnerability:** Virtual machine log files do not have a size limit.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record Retention

**Categories:** 10.2 Content Configuration

**Responsibility:** Information Assurance Officer / System Administrator

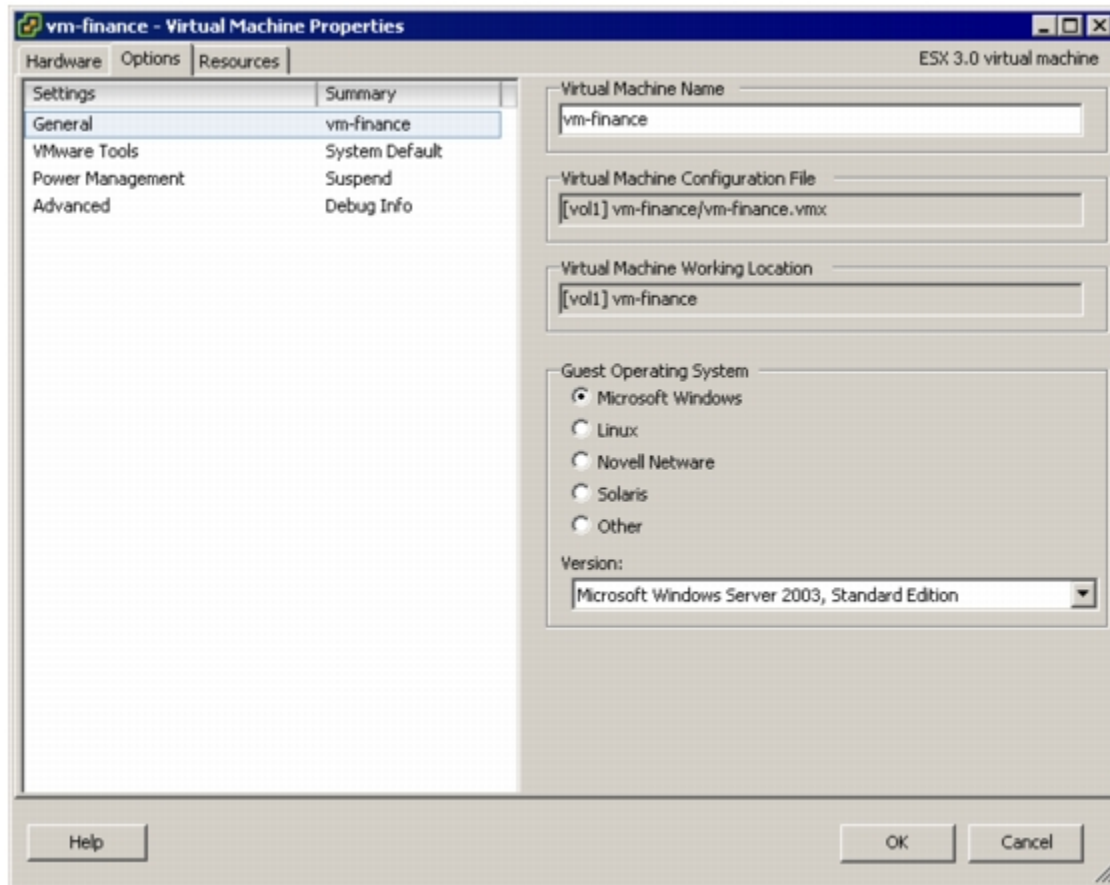
**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines can write troubleshooting information into a virtual machine log file (vmware.log) stored on the VMFS volume. Virtual machine users and processes may be configured to abuse the logging function, either intentionally or inadvertently so that large amounts of data flood the log file. Over time, the log file can consume so much of the ESX Server's file system space that it fills the hard disk, causing an effective denial of service on the ESX Server.

**Computing Check:**

1. Login to VirtualCenter with the VI Client and select the virtual machine from the inventory panel.  
The configuration page for the virtual machine appears with the Summary tab displayed.
2. Click Edit Settings.
3. Click Options > General and make a record of the path displayed in the virtual machine configuration file field.



4. At the ESX Server service console, change directories to access the virtual machine configuration file recorded in step 3.
5. Virtual machine configuration files are located in the /vmfs/volumes/<datastore> directory, where (datastore) is the name of the storage device on which the virtual machine files reside. In example above, [vol1]vm-finance/vm-finance.vmx is located in /vmfs/volumes/vol1/vm-finance/.
6. To verify the log size limit, perform the following:  
#cat (virtual machine name).vmx | grep log.rotateSize  
log.rotateSize=(number in bytes)

If no limit is set, then this is a finding. The default is 500KB.

**Fix:** Configure a limit for virtual machine log size.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1120:** ESX Server is not configured to maintain a specific number of log files

**Vulnerability Key:** V0015908

**STIG ID:** ESX1120

**Vulnerability:** ESX Server is not configured to maintain a specific number of log files via log rotation.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record Retention

**Categories:** 10.2 Content Configuration

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines can write troubleshooting information into a virtual machine log file (vmware.log) stored on the VMFS volume. Virtual machine users and processes may be configured to abuse the logging function, either intentionally or inadvertently so that large amounts of data flood the log file. Over time, the log file can consume so much of the ESX Server's file system space that it fills the hard disk, causing an effective denial of service on the ESX Server.

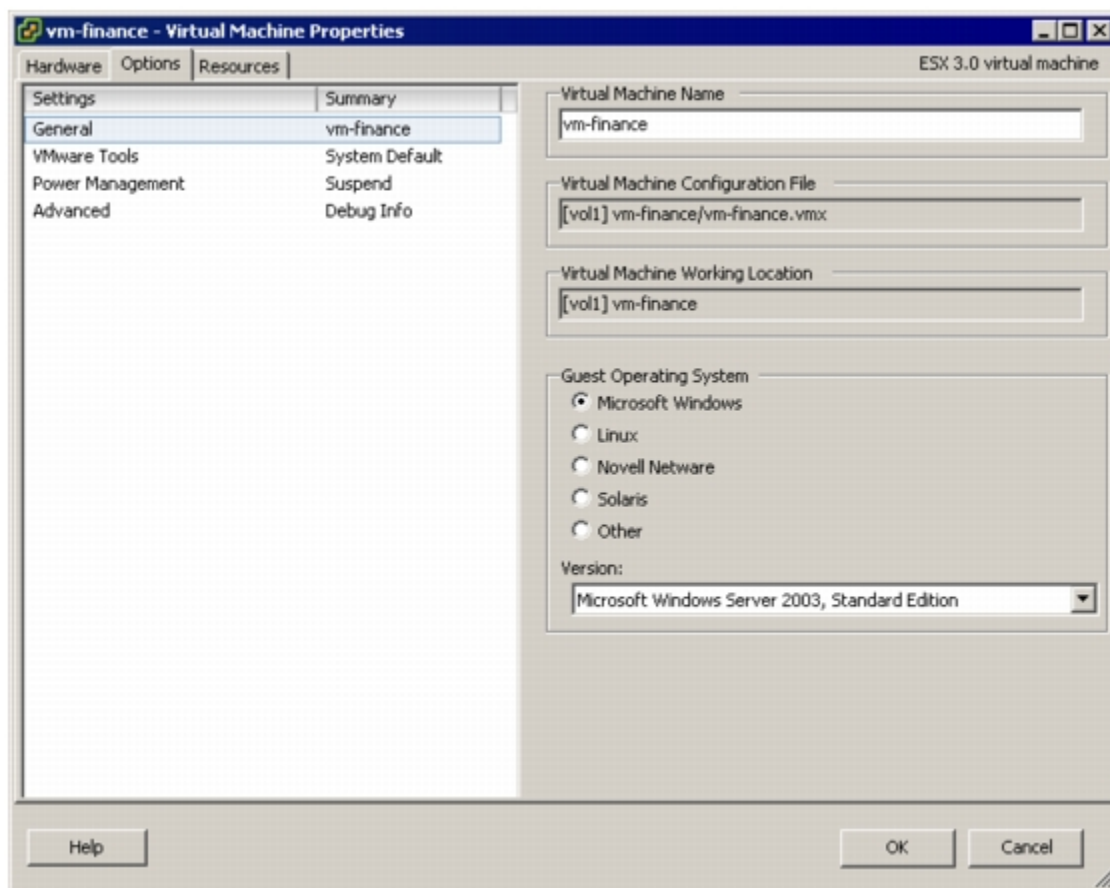
**Computing Check:**

1. Login to VirtualCenter with the VI Client and select the virtual machine from the inventory panel.

The configuration page for the virtual machine appears with the Summary tab displayed.

2. Click Edit Settings.

3. Click Options > General and make a record of the path displayed in the virtual machine configuration file field.



4. At the ESX Server service console, change directories to access the virtual machine configuration file recorded in step 3.
5. Virtual machine configuration files are located in the /vmfs/volumes/<datastore> directory, where <datastore> is the name of the storage device on which the virtual machine files reside. In example above, [vol1]vm-finance/vm-finance.vmx is located in /vmfs/volumes/vol1/vm-finance/.
6. To verify the number of log files has been configured, perform the following:  
#cat <virtual machine name>.vmx | grep log.keepOld  
If log.keepOld=<number of files to keep> is not configured to 6 or higher, then this is a finding. The default number of files to keep is 6 where the oldest ones are deleted and new ones are created.

**Fix:** Configure the ESX Server to limit the number of logs retained.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1130:** Virtual machine log files are not retained for 1 year

**Vulnerability Key:** V0015909

**STIG ID:** ESX1130

**Vulnerability:** Virtual machine log files are not maintained for 1 year.

**IA Controls:** ECAR-1, ECAR-2, ECAR-3 Audit Record Retention

**Categories:** 10.5 Retention

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Storing log files for at least a year provides a way to recover these files in case an investigation is necessary. Typically these files are stored offline on tape media or external networks. Log files enable the enforcement of individual accountability by creating a reconstruction of events. They also assist in problem identification that may lead to problem resolution. If these log files are not retained, there is no way to trace or reconstruct the events, and if it was discovered the network was hacked, there would be no way to trace the full extent of the compromise.

**Computing Check:** Locate where archived virtual machine log files (vmware.log) are stored. If they are offsite, review the process to move them to this alternative site. Verify that the log files are retained for at least one year at a minimum. This can be verified by reviewing the dates of the oldest backup files or media. If the log files are not stored for a minimum of one year, then this is a finding.

**Fix:** Retain virtual machine log files for a minimum of one year.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1140:** Virtual machines are not backed up

**Vulnerability Key:** V0015913

**STIG ID:** ESX1140

**Vulnerability:** Virtual machines are not backed up in accordance with the MAC level.



**IA Controls:** CODB-1, CODB-2, CODB-3 Data Backup

**Categories:** 13.4 Backup and Recovery

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Backups of the virtual machines are critical in order to recover from hardware problems, unexpected software errors, or a disaster to the computing facility. Data backup must be performed in accordance with its mission assurance category (MAC) level. For MAC III systems it is necessary to ensure that backups are performed weekly. For MAC II systems backups are performed daily and the recovery media is stored off-site in a protected facility in accordance with its mission assurance category and confidentiality level. In MAC I systems backups are maintained through a redundant secondary system which is not collocated, and can be activated without loss of data or disruption to the operation.

**Computing Check:**

1. Determine the MAC level of the virtual machines by asking the IAO/SA.
2. Once the MAC level is determined, locate the backup media or storage location.  
For MAC I servers, a redundant secondary system is required that is not collocated.  
For MAC II servers, daily backups are required with recovery media stored offline.  
For MAC III servers, backups must be performed weekly.
3. Depending on the MAC level, verify the virtual machines are backed up to media or storage within the guidelines of the MAC level. If they are not, then this is a finding.

**Fix:** Backup all virtual machines according to the MAC level.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1150:** Virtual machines are not registered in VMS

**Vulnerability Key:** V0015972

**STIG ID:** ESX1150

**Vulnerability:** Virtual machines are not registered in VMS.

**IA Controls:** VIVM-1 Vulnerability Management

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Running the most current, approved version of software on all virtual machines will help maintain a stable base of security fixes as well as security enhancements. Virtual machines that are not running the latest tested and approved versions of software are vulnerable to the potential attacks. Furthermore, if the virtual machine is no longer supported by the vendor, patches will not be made available to address weaknesses exposing new vulnerabilities, nor will IAVM notices be made available that provide announcements of these new vulnerabilities along with measures to mitigate their associated risks.

**Computing Check:** Use VMS and navigate to the site's assets. Ensure all virtual machines are registered within VMS. If they are not registered, this is a finding.

**Fix:** Register all virtual machines in VMS.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

#### 4. GUEST ADMINISTRATOR CHECKLIST

The Guest Administrator role is responsible for managing a guest virtual machine or machines. Tasks that are typically performed by Guest Administrators are connecting virtual devices, system updates, and applications that may reside on the operating system.

**ESX1160:** Virtual machine requirements are not documented

**Vulnerability Key:** V0015919

**STIG ID:** ESX1160

**Vulnerability:** Virtual machine requirements are not documented before creating virtual machine.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.9 Documentation

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category III

**Vulnerability Discussion:** Guest operating systems may require different resources depending on the server function. A database or email server will require more resources than a basic Windows Domain Controller. Therefore, proper planning is required to determine what servers will be built within the virtualization server environment.

To properly create virtual machines within the virtualization server environment, a minimal list of requirements will be determined. These requirements are the amount of memory, amount of required disk space, the networking card assignment, required media, and proper disk mode to be used.

**Non-Computing Check:** Request a copy of the virtual machine requirements documentation. If no documentation exists, then this is a finding.

**Fix:** Develop virtual machine requirements documentation.

Comments:

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1170:** Unused hardware is enabled in virtual machines

**Vulnerability Key:** V0015921

**STIG ID:** ESX1170

**Vulnerability:** Unused hardware is enabled in virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines can connect or disconnect hardware devices. These devices may be network adapters, CD-ROM drives, USB drives, etc. Attackers may use this capability via non-privileged users or processes to breach virtual machines in several ways. An attacker that has access to a virtual machine may connect a CD-ROM drive and access sensitive information on the media left in the drive. Another action an attacker may perform is disconnecting the network adapter to isolate the virtual machine from its network resulting in a denial of service. Therefore, as a general security precaution, SAs will remove any unneeded or unused hardware devices. If permanently removing a device is not feasible, SAs can restrict a virtual machine process or user from connecting or disconnecting devices from within the guest operating system.

**Computing Check:**

1. Login to VirtualCenter with the VI Client and select the virtual machine from the inventory panel.
2. Click Edit settings.
3. Click the Hardware tab.
4. Compare the virtual machine requirements documentation for the virtual machine to ensure that only the required devices are configured in the hardware tab. All devices (serial ports, network adapters, CD-ROMs, etc.) that are listed in the hardware tab and not in the virtual machine documentation will be a finding. If no virtual machine requirements exist, then this is a finding.

**Fix:** Disable or remove all unused hardware in virtual machines.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1180:** Guest operating system selection does not match installed OS

**Vulnerability Key:** V0015924

**STIG ID:** ESX1180

**Vulnerability:** Guest operating system selection does not match installed OS.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Selecting the correct guest operating system for each virtual machine is important. ESX Servers optimize certain internal configurations on the basis of this selection. For this reason, it is important to set the guest operating system correctly. The correct guest operating selection can greatly aid the operating system chosen and may cause significant performance degradation if there is a mismatch between the selection and the operating system actually running in the virtual machine. The performance degradation may be similar to running an unsupported operating system on the ESX Server. Selecting the wrong guest operating system is not likely to cause a virtual machine to run incorrectly, but it could degrade the virtual machine's performance.

**Computing Check:**

Select a Linux and Windows server to verify that the OS selections are accurate. For instance, Red Hat EL 4 should be selected as RedHat EL 4, not Linux, Suse, etc.

1. Login to VirtualCenter with the VI Client and select the virtual machine from the inventory panel.
2. Click Edit settings. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.
3. Review the selected OS and the actual OS running. If they are different, then this is a finding.

**Fix:** Select the correct operating system for all virtual machines.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1190:** Guest operating system is not supported by ESX Server

**Vulnerability Key:** V0015926

**STIG ID:** ESX1190

**Vulnerability:** Guest operating system is not supported by ESX Server.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.8 Unsupported Vendor Products

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

## Severity: Category I

**Vulnerability Discussion:** The guest operating systems on the ESX Server must be supported by VMware. Guest operating systems will need to be approved by VMware so that if problems are encountered with the guest operating system, then VMware can assist with the resolution. Also, unsupported guest virtual machines create problems since no documentation or support is available from VMware.

## Computing Check:

The following table lists the supported operating systems for each VMware product. For the ESX Server, focus on column 4 in the Table. If the table has a blank box, this means the operating system is not supported.

1. Login to VirtualCenter with the VI Client. Select an ESX Server and review all the virtual machines.
2. Review the OS of the virtual machines and verify that no “other” virtual machines are running. If so, then this is a finding.

Guest Operating System	Workstation	VMware ACE	GSX Server	ESX Server	VMware Server	VMware Fusion
Windows Server 2008	6.0.1–6.0.2	2.0.1–2.0.2		3.5		
Windows Vista	6.0–6.0.2	2.0–2.0.2		3.0–3.5		1.0–1.1.1
Windows Server 2003	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–3.5	1.0–1.0.4	1.0–1.1.1
Windows XP	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–3.5	1.0–1.0.4	1.0–1.1.1
Windows 2000	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–3.5	1.0–1.0.4	1.0–1.1.1
Windows NT 4.0	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–3.5	1.0–1.0.4	1.0–1.1.1
Windows Me	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	1.0–1.1.1

Windows 98	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	1.0–1.1.1
Windows 95	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	1.0–1.1.1
DOS and Windows 3.1x	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	1.0–1.1.1
Mandriva Corporate Server 4	5.5.3–6.0.2	2.0–2.0.2				
Mandriva Linux 2007	5.5.3–6.0.2	2.0–2.0.2				1.0–1.1.1
Mandriva Linux 2006	5.5.2–6.0.2	2.0–2.0.2			1.0–1.0.4	1.0–1.1.1
Mandrake Linux 10.1	5.5–6.0.2	2.0–2.0.2	3.2–3.2.1		1.0–1.0.4	
Mandrake Linux 10	5.0–6.0.2	2.0–2.0.2	3.2–3.2.1		1.0–1.0.4	
Mandrake Linux 9.2	5.0–6.0.2	2.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Mandrake Linux 9.1			3.1–3.2.1			
Mandrake Linux 9.0	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Mandrake Linux 8.2	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Mandrake Linux 8.0 and 8.1			3.0–3.2.1			

Novell Linux Desktop 9	5.0–6.0.2	1.0–2.0.2			1.0–1.0.4	1.0–1.1.1
Red Hat Enterprise Linux 5	5.5.3–6.0.2	2.0–2.0.2		3.0.2–3.5		1.0–1.1.1
Red Hat Enterprise Linux 4	5.0–6.0.2	1.0.1–2.0.2	3.2–3.2.1	2.5.2–3.5	1.0–1.0.4	1.0–1.1.1
Red Hat Enterprise Linux 3	4.5–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0.1–3.5	1.0–1.0.4	1.0–1.1.1
Red Hat Enterprise Linux 2.1	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–3.5	1.0–1.0.4	1.0–1.1.1
Red Hat Linux 9.0	4.0.1–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–2.5.5	1.0–1.0.4	1.0–1.1.1
Red Hat Linux 8.0	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–2.5.5	1.0–1.0.4	
Red Hat Linux 7.3	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–2.5.5	1.0–1.0.4	
Red Hat Linux 7.2	4.0–6.0.2	1.0.2.0.2	3.0–3.2.1	2.0–2.5.5	1.0–1.0.4	
Red Hat Linux 7.1	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Red Hat Linux 7.0	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	1.0–1.1.1
Red Hat Linux 6.2			3.0–3.2.1			
Sun Java Desktop System 2	5.0–6.0.2	2.0–2.0.2			1.0–1.0.4	



SUSE Linux Enterprise Server 10	5.5.2–6.0.2	2.0–2.0.2		3.0.1–3.5	1.0–1.0.4	1.0–1.1.1
SUSE Linux Enterprise Server 9	5.0–6.0.2	1.0.1–2.0.2	3.2–3.2.1	2.5–3.5	1.0–1.0.4	
SUSE Linux Enterprise Server 8	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–3.5	1.0–1.0.4	
SUSE Linux Enterprise Server 7	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Open SUSE Linux 10.3	6.0.1–6.0.2	2.0.1–2.0.2				
Open SUSE Linux 10.2	6.0–6.0.2	2.0–2.0.2				
SUSE Linux 10.1	5.5.2–6.0.2	2.0–2.0.2			1.0–1.0.4	1.0–1.1.1
SUSE Linux 10	5.5–6.0.2	2.0–2.0.2			1.0–1.0.4	
SUSE Linux 9.3	5.5–6.0.2	2.0–2.0.2		2.5.2–2.5.5	1.0–1.0.4	1.0–1.1.1
SUSE Linux 9.2	5.0–6.0.2	1.0.1–2.0.2	3.2–3.2.1	2.5.1–2.5.5	1.0–1.0.4	
SUSE Linux 9.1	4.5.2–6.0.2	1.0–2.0.2	3.1–3.2.1	2.5–2.5.5	1.0–1.0.4	
SUSE Linux 9.0	4.5–6.0.2	1.0–2.0.2	3.0–3.2.1	2.1–2.5.5	1.0–1.0.4	
SUSE Linux 8.2	4.0.1–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0–2.5.5	1.0–1.0.4	

SUSE Linux 8.1	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
SUSE Linux 8.0	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
SUSE Linux 7.3	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Turbolinux 10 Server	6.0.1–6.0.2	2.0.1–2.0.2				
Turbolinux 10 Desktop	5.5–6.0.2	2.0–2.0.2			1.0–1.0.4	1.0–1.1.1
Turbolinux Enterprise Server 8	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	1.0–1.1.1
Turbolinux Workstation 8	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Turbolinux 7.0	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Ubuntu Linux 7.04	6.0–6.0.2	2.0–2.0.2		3.0.2–3.5		
Ubuntu Linux 6.10	6.0–6.0.2	2.0–2.0.2				1.0–1.1.1
Ubuntu Linux 6.06	5.5.2–6.0.2	2.0–2.0.2			1.0–1.0.4	
Ubuntu Linux 5.10	5.5–6.0.2	2.0–2.0.2			1.0–1.0.4	1.0–1.1.1
Ubuntu Linux 5.04	5.5–6.0.2	2.0–2.0.2			1.0–1.0.4	

FreeBSD 6.2	6.0.1–6.0.2	2.0.1– 2.0.2				
FreeBSD 6.1	5.5.2–6.0.2	2.0–2.0.2				1.0–1.1.1
FreeBSD 6.0	5.5.2–6.0.2	2.0–2.0.2			1.0–1.0.4	
FreeBSD 5.5	5.5–6.0.2	2.0– 2.0.22			1.0–1.0.4	1.0–1.1.1
FreeBSD 5.4	5.5–6.0.2	2.0–2.0.2			1.0–1.0.4	
FreeBSD 5.3	5.5–6.0.2	2.0–2.0.2			1.0–1.0.4	
FreeBSD 5.2	5.0–6.0.2	2.0–2.0.2	3.1– 3.2.1		1.0–1.0.4	
FreeBSD 5.1	5.0–6.0.2	2.0–2.0.2	3.2– 3.2.1		1.0–1.0.4	
FreeBSD 5.0	4.5–6.0.2	1.0–2.0.2	3.0– 3.2.1		1.0–1.0.4	
FreeBSD 4.11				2.5.4– 2.5.5		
FreeBSD 4.10				2.5– 2.5.5		
FreeBSD 4.9			3.2– 3.2.1	2.5		
FreeBSD 4.4, 4.5, 4.6.2, 4.8	4.0–6.0.2	1.0–2.0.2	3.0– 3.2.1		1.0–1.0.4	

FreeBSD 4.0, 4.1, 4.2, 4.3	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
NetWare 6.5 Server	4.5–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0.1–3.5	1.0–1.0.4	1.0–1.1.1
NetWare 6.0 Server	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0.1–3.5	1.0–1.0.4	
NetWare 5.1 Server	4.0–6.0.2	1.0–2.0.2	3.0–3.2.1	2.0.1–3.5	1.0–1.0.4	
NetWare 4.2 Server	5.5.2–6.0.2	2.0–2.0.2	3.0–3.2.1		1.0–1.0.4	
Solaris 10 Operating System for x86 Platforms	4.5.2–6.0.2	1.0–2.0.2	3.1–3.2.1	3.0–3.5	1.0–1.0.4	1.0–1.1.1
Solaris 9 Operating System x86 Platform Edition	4.5.2–6.0.2	1.0–2.0.2	3.1–3.2.1		1.0–1.0.4	

**Fix:** Use only supported operating systems on the ESX Server.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	

**ESX1200:** Anti-virus software and signatures are out of date for off and suspended virtual machines.

**Vulnerability Key:** V0015931

**STIG ID:** ESX1200

**Vulnerability:** Anti-virus software and signatures are out of date for off and suspended virtual machines.

**IA Controls:** ECVF-1 Anti-virus software

**Categories:** 14.7 Antivirus

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Creating new virtual machines is as easy as copying a file. Copying files is a quick and efficient way to rollout new virtual machines. Virtual machines can grow at an explosive rate and really tax the security systems of an organization. Many administrative tasks may be automated, but some upgrades and patches require manual tools. For instance, virtual machines may need to be patched, scanned, and purged in response to a virus or worm attack on the network. Therefore, to protect against potential virus and spyware infections, all off and suspended virtual machines will have the latest up-to-date anti-virus software and signatures.

**Computing Check:**

Work with the OS reviewer to determine if the requirement is being met.

1. Login to VirtualCenter with the VI Client and select a suspended or off virtual machine.
2. Turn on the virtual machine and have the IAO/SA login.
3. Obtain the running virus engine and signatures from guest operating system and compare this with the latest virus engine and signatures released from the JTG-GNO. URL for JTG-GNO is [https://www.jtfgno.mil/antivirus/av\\_info.htm](https://www.jtfgno.mil/antivirus/av_info.htm). If the signature or engine is older than the latest release, then this is a finding.

**Fix:** Maintain the latest virus updates for all off and suspended virtual machines.

Comments:

Finding		Not a Finding		Not Reviewed		Not Applicable	
---------	--	---------------	--	--------------	--	----------------	--

**ESX1210:** OS patches and updates are out of date on off and suspended virtual machines

**Vulnerability Key:** V0015932

**STIG ID:** ESX1210

**Vulnerability:** OS patches and updates are out of date on off and suspended virtual machines.

**IA Controls:** ECSC-1 Security Configuration Compliance

**Categories:** 12.4 CM Process

**Responsibility:** Information Assurance Officer / System Administrator

**References:** ESX Server STIG

**Severity:** Category II

**Vulnerability Discussion:** Virtual machines create a condition where they may be on, off, or suspended. The requirement that machines be on in a conventional approach to patch management, virus and vulnerability scanning, and machine configuration creates an issue in the virtual world. Virtual machines can appear and disappear from the network sporadically. Conventional networks can “anneal” new machines into a known good configuration state very quickly. However, converging virtual machines to a known good state is more challenging since the state may change quickly. For instance, a vulnerable machine can appear briefly and either become infected or reappear in a vulnerable state at a later time. Therefore, vulnerable virtual machines may become infected with a virus and never be detected since the virtual machine may be suspended or off. Suspended and off virtual machines should be patched regularly to ensure patches are up to date. Virtual machines that are on will be kept current with the operating system patches per the appropriate OS STIG.

**Computing Check:**

Work with the OS reviewer to determine if the requirement is being met.

1. Login to VirtualCenter with the VI Client and select a suspended or off virtual machine.
2. Turn on the virtual machine and have the IAO/SA login.
3. Have the IAO/SA obtain the latest patch level for the OS and compare this to the latest release from the OS vendor. If the patch level is older than the latest release, then this is a finding.

**Fix:** Keep all suspended and off virtual machines patched.

Comments:							
Finding		Not a Finding		Not Reviewed		Not Applicable	